ENHWI-G

IEEE 802.11g
Wireless Broadband Router

User Guide

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

·On board of airplanes, or

·In an explosive environment, or

·In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and

2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons has to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the distance between the equipment and the receiver.
3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US of Canada without an approved US Department of Commerce export license.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

TABLE OF CONTENT

ABOUT THIS GUIDE 1

Purpose 1

Overview of this User's Guide 1

INTRODUCTION 2

Applications: 2

Features: 3

UNPACKING AND SETUP 4

Unpacking 4

Setup 4

HARDWARE INSTALLATION 5

Front Panel 5

Rear Panel 5

Hardware connections 6

Connect the Router using LAN 6

Connect the Router using Wireless LAN 7

Check the installation 7

PC NETWORK TCP/IP SETTING 8

Windows 95/98/ME 8

Windows 2000 9

Windows XP 10

WIRELESS BROADBAND ROUTER CONFIGURATION 11

Login to the Wireless Broadband Router through WLAN 11

Login to the Wireless Broadband Router through LAN 11

Using the Web Browser 11

Quick Setup 12

Advance Setup 20

2.1 LAN Setting 20

2.1.1 LAN & DHCP Server 20

2.1.2 WAN 21

2.1.3 Password 22

2.1.4 Time 23

2.2 Wireless 24

2.2.1 Basic 24
2.2.2 Authentication 25
2.2.3 Advanced 27
2.3 Status 27
2.3.1 Device Information 28
2.3.2 Log 28
2.3.3 Log Setting 30
2.3.4 Statistic 31
2.3.5 Wireless 32
2.4 Routing 33
2.4.1 Static 33
2.4.2 Dynamic 34
2.4.3 Routing Table 35
2.5 Access 36
2.5.1 MAC Filters 36
2.5.2 Protocol Filter 37
2.5.3 IP Filter 37
2.5.4 Virtual Server 39
2.5.5 Special AP 40
2.5.6 DMZ 41
2.5.7 Firewall Rule 42
2.6 Management 44
2.6.1 Remote Management 44
2.7 Tools 45
2.7.1 Reset 45
TECHNICAL SPECIFICATIONS 49

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11g Wireless Broadband Router. This integrated access device combines Internet gateway functions with wireless LAN and Fast Ethernet switch. It provides a complete solution for Internet surfing and office resources sharing, and it is easy to configure and operate for every users.

Purpose

This manual discusses how to install the IEEE 802.11g Wireless Broadband Router.

Overview of this User's Guide

Introduction. Describes the Wireless Broadband Router and its features.

Unpacking and Setup. Helps you get started with the basic installation of the Wireless Router.

Identifying External Components. Describes the front panel, rear panel and LED indicators of the Wireless Router.

Connecting the Router. Tells how you can connect the Wireless Router to your xDSL/Cable Modem.

Technical Specifications. Lists the technical (general, physical and environmental, performance and Routers settings) specifications of the Wireless Broadband Router.

INTRODUCTION

With the explosive growth of the Internet, accessing information and services at any time, day or night has become a standard requirement for most people. The era of the standalone PC is waning. Networking technology is moving out of the exclusive domain of corporations and into homes with at least two computers.

This integrated access device combines Internet gateway functions with wireless LAN and Fast Ethernet switch. Designed for the business and home, it saves you the cost of installing a separate modem and ISP line for each computer, while providing ready connection for the users, with or without the network wires.

Broadband network access is also gaining ground. However, allowing more than two computers to access the Internet at the same time means less affordable, higher costs. Thus, there is a need to share one legal IP address over a single Internet connection to link the home with the Internet.

The scarcity of IP addresses and using a shared Internet connection through an Internet sharing device can solve high network access costs. All linked computers can make full use of broadband capabilities over such a device.

This device not only comes equipped with a wide range of features, but also can be installed and configured right out of the box. This device supports a simple local area network and Internet access share, offering great cost savings.

The local area network connects up home computers while also allowing any of the computers to access the Internet, share resources, or play online games—the basis of the family computing lifestyle.

Applications:

Broadband Internet access:

Several computers can share one high-speed broadband connection through wireless or wired (WLAN, LAN and WAN-Internet).

Resource sharing:

Share resources such as printers, scanners and other peripherals.

File sharing:

Exchange data, messages, and distribute files thus making good use of hard disk space.

Online gaming:

Through the local area network, online gaming and e-commerce services can be easily setup.

Firewall:

A built-in firewall function — for security and anti-hack system.

Features:

- High speed data transfer rate
- Supports NAT for share 1 IP address to all LAN user.
- Supports PPPoE and PPTP protocol for Dial-Up ADSL.
- Supports 64/128 bit WEP Encryption
- Supports WPA security
- Supports DHCP Server / Client.
- Supports UPnP (Universal Plug and Play).
- Supports virtual server mapping.
- Supports packet filtering.
- Supports DNS
- Simple Firewall protection.
- Upgradeable firmware for future function.
- Simple setting using Quick Setup.
- Easy configuration via WEB Browser.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Wireless Broadband Router.

Unpacking

Open the box of the Wireless Broadband Router and carefully unpack it. The box should contain the following items:

- One Wireless Internet Broadband Router
- One external power adapter
- One CD-Rom with this User's Guide

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

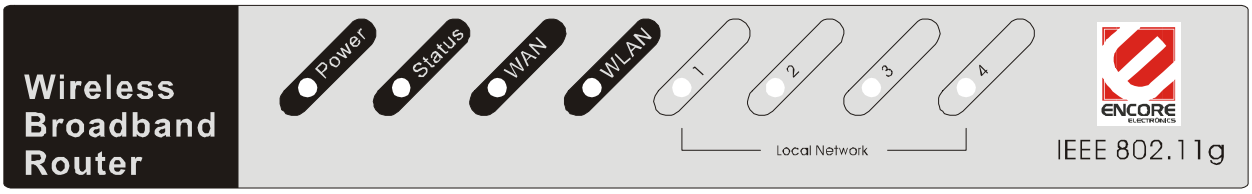
The setup of the Wireless Broadband Router can be performed properly using the following methods:

- The power outlet should be within 1.82 meters (6 feet) of the Broadband Router.
- Visually inspect the DC power jack and make sure that it is fully secured to the power adapter.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Broadband Router. Do not place heavy objects on the Broadband Router.
- Fix the direction of the antennas. Try to place the Wireless Router in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.

HARDWARE INSTALLATION

Front Panel

The figure below shows the front panel of the Wireless Broadband Router.



Wireless Broadband Router Front Panel

POWER

This indicator lights green when the hub is receives power, otherwise it is off.

SYSTEM

This indicator blinks green means the Internet Broadband Router is working successful. Otherwise, this indicator always on or off means the function of the Internet Broadband Router is fail.

WAN (Link/ACT)

The indicators light green when the WAN port was connected to an xDSL/Cable modem successfully.

The indicators blink green while the WAN port was transmitting or receiving data on the xDSL/Cable modem.

WLAN (ACT)

This indicator lights green when there are wireless devices connected and transmitting data to the Wireless Router.

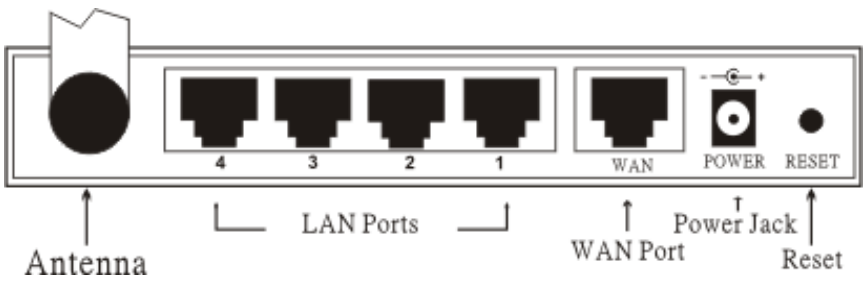
LAN (Link/ACT)

These indicators light green when the LAN ports were connected successfully.

These indicators blink green while the LAN ports were transmitting data.

Rear Panel

The figure below shows the rear panel of the Wireless Broadband Router.



Wireless Broadband Router Rear Panel

Antenna

There are two 2 dBi Gain Antenna in the rear panel for wireless connection.

LAN (1-4)

Four RJ-45 10/100Mbps Auto-MDIX ports for connecting to either 10Mbps or 100Mbps Ethernet connections.

WAN

In the four port broadband router, there is an RJ-45 10/100Mbps Auto-MDIX port for the WAN that will fit the xDSL/Cable modem's specification need.

DC IN

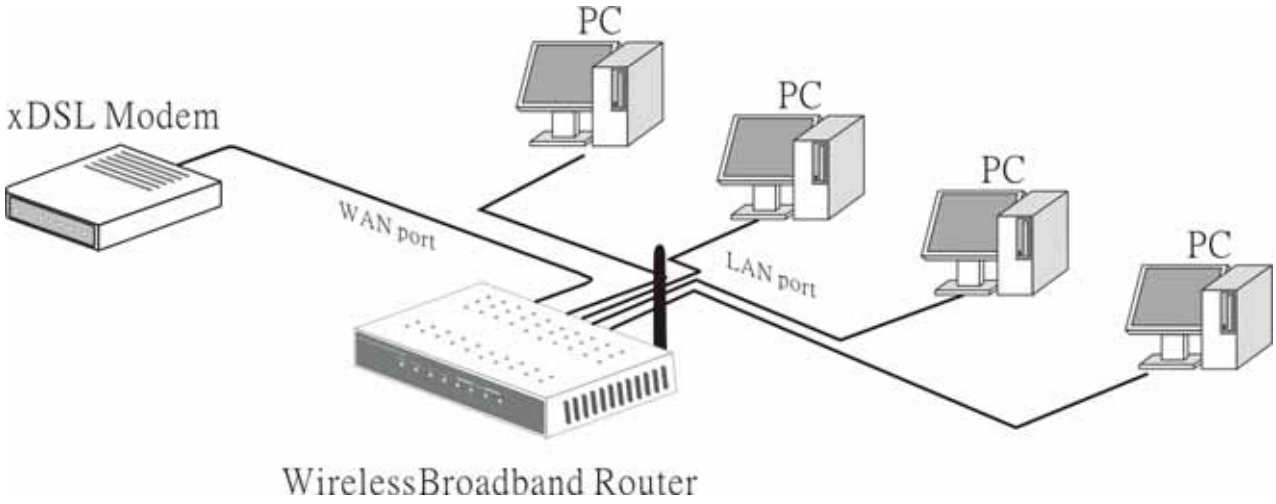
Plug the power adapter to this power jack

RESET

Use a pin-shape item to push to reset this device to factory default settings. It will be useful too when the manager forgot the password to login, but the setting will be back to default setting.

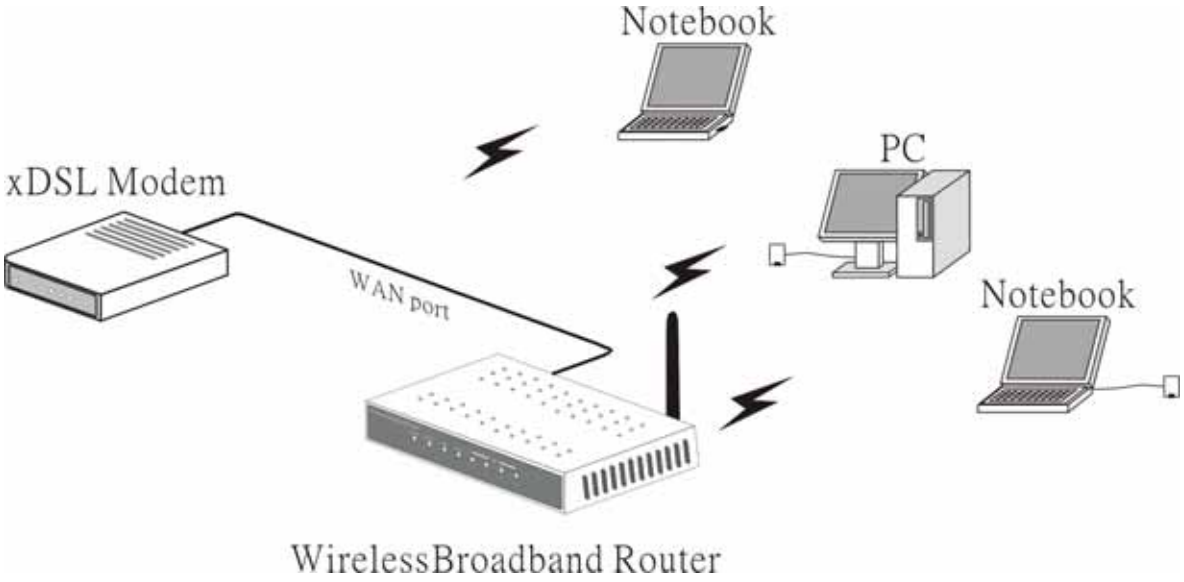
Hardware connections

Connect the Router using LAN



1. Plug in one end of the network cable to the WAN port of the Wireless Internet Broadband Router.
2. Plug in the other end of the network cable to the Ethernet port of the xDSL or Cable modem.
3. Use another network cable to connect to the Ethernet card on the computer system; the other end of the cable connects to the LAN port of the Internet Broadband Router. Since the Wireless Broadband Router has four ports, you can connect up to four computers directly to the unit. There you do not have to buy a switch to connect these computers since one Internet Broadband Router functions both as a connection-sharing unit and as a switch.

Connect the Router using Wireless LAN



1. Plug in one end of the RJ45 network cable to the xDSL/Cable Modem.
2. Plug in the other end of the RJ45 network cable to the Wireless Internet Broadband Router WAN port.

Check the installation

The control LEDs of the Wireless Internet Broadband Router are clearly visible and the status of the network link can be seen instantly:

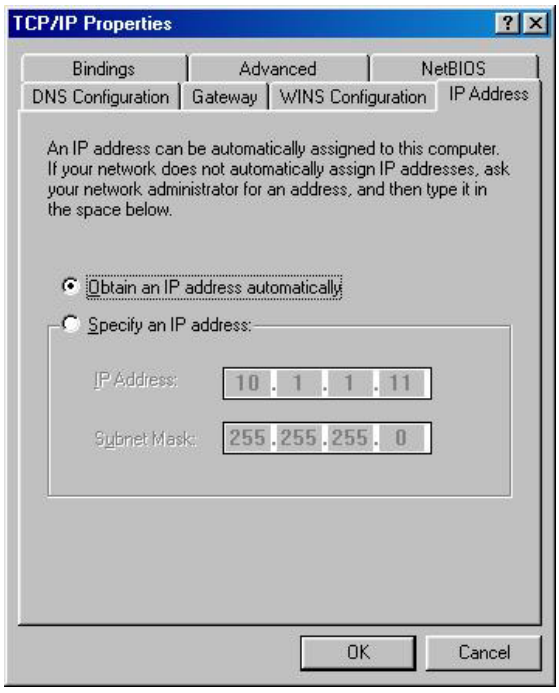
1. With the power source on, once the device is connected to the broadband modem, the Power, CPU, LAN, WLAN and WAN port link LEDs of the Internet Broadband Router will light up indicating a normal status.
2. While the WAN is link up to the ADSL/Cable modem, the WAN port's Link/ACT LED will light up.
3. While the LAN is link up to the computer system, the LAN port's Link/ACT LED will light up.

PC NETWORK TCP/IP SETTING

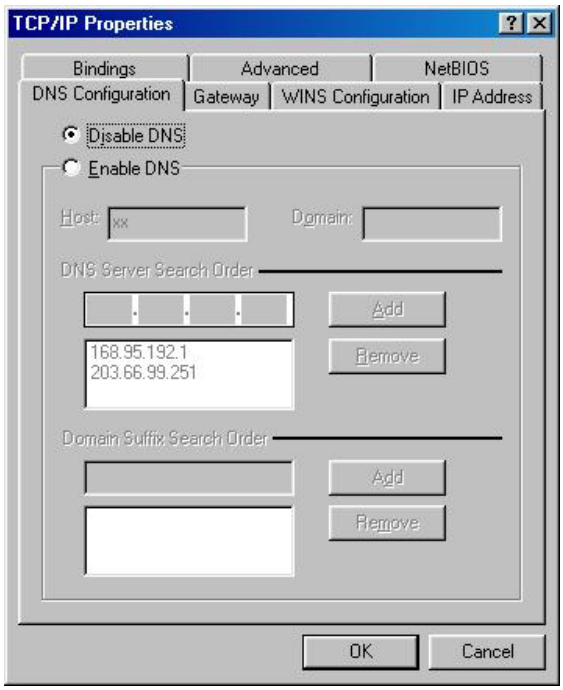
The network TCP/IP settings differ based on the computer's operating system (Win95/98/ME/NT/2000/XP) and are as follows.

Windows 95/98/ME

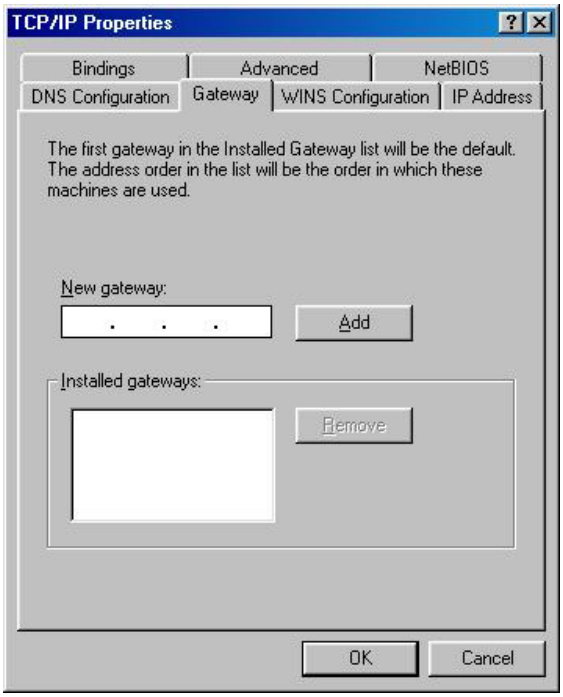
1. Click on the "**Network neighborhood**" icon found on the desktop.
2. Click the right mouse button and a context menu will be show.
3. Select "**Properties**" to enter the TCP/IP setting screen.
4. Select "**Obtain an IP address automatically**" on the "**IP address**" field.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
10 . 1 . 1 . 11
Subnet Mask:
255 . 255 . 255 . 0
OK
Cancel

5. Select "**Disable DNS**" in the "**DNS**" field.



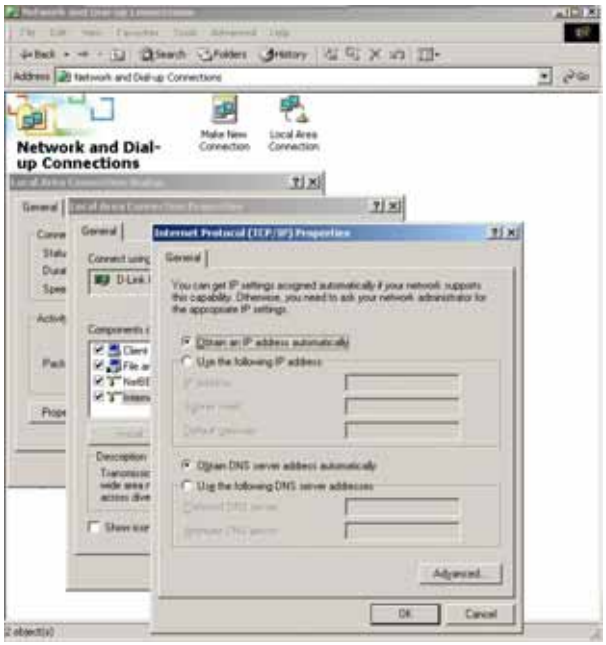
6. Select “**None**” for the “**Gateway address**” field.



Windows 2000

Double click on the “**My computer**” icon on the desktop. When “**My computer**” window opens, open the “**Control panel**” and then open the “**Network dialup connection**” applet. Double click on the “Local area network connection” icon. Select “Properties” to enter the TCP/IP setting window.

1. In the “**Local area network status**” window, click on “**Properties**.”
2. In the “**Local area network connection**” window, first select TCP/IP setting and then select “**Properties**.”
3. Set both “**IP address**” and “**DNS**” to **Automatic configuration**.

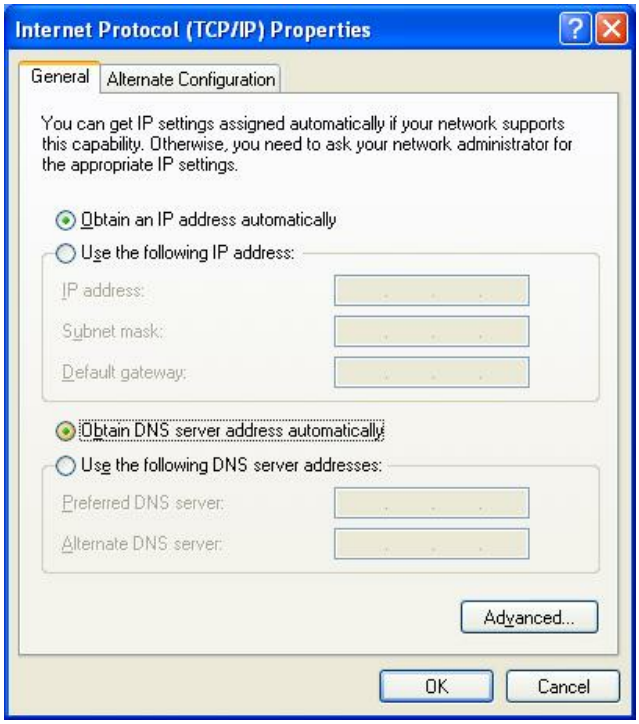


Windows XP

Point the cursor and click the right button on the “My Network Place” icon.

Select “properties” to enter the TCP/IP setting window.

1. Set “**IP address**” to “**Obtain an IP address automatically**.”
2. Set “**DNS**” to “**Obtain DNS server address automatically**.”


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

WIRELESS BROADBAND ROUTER CONFIGURATION

First make sure that the network connections are functioning normally.

This Wireless Broadband Router can be configured using Internet Explorer 4.0 or newer web browser versions.

Login to the Wireless Broadband Router through WLAN

Before configuring the Wireless Broadband Router through WLAN, make sure that the SSID, Channel and the WEP is set properly.

The default setting of the Wireless Broadband Router that you will use:

SSID: default

Channel: 6

Security: disable

Login to the Wireless Broadband Router through LAN

Before you configure this device, note that when the Wireless Broadband Router is configured through an Ethernet connection, make sure the host PC must be set on the **IP subnetwork** that can be accessed by the xDSL/Cable modem. For example, when the default network address of the xDSL/Cable modem Ethernet interface is 192.168.1.x, then the host PC should be set at 192.168.1.xxx (where xxx is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Using the Web Browser

1. Open Internet Explorer 4.0 or above Internet browser.
2. Enter IP address ***http://192.168.1.1*** (the factory-default IP address setting) to the URL web address location.

3. When the following dialog box appears, enter the user name and password to login to the main configuration window, the default username and password is "***admin***".

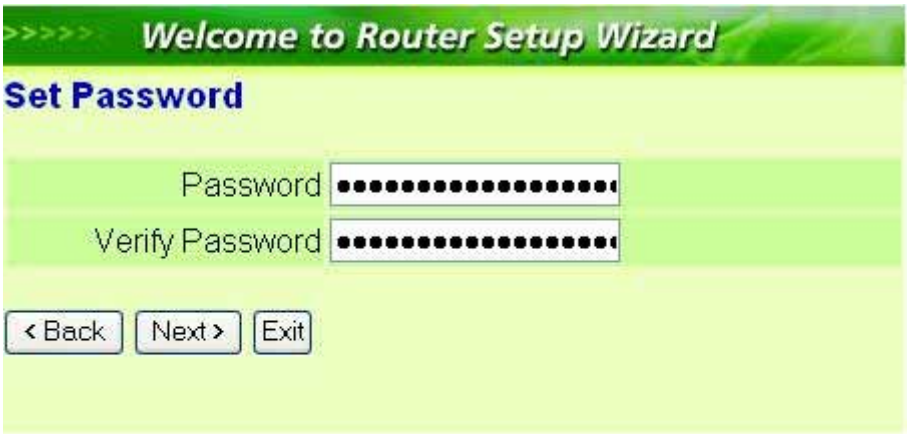
Note: If needed to set a password, then refer to the **Main Page Password Setting**.

Quick Setup

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get the wireless router configuration ready to run in 6 easy steps by clicking on the “Wizard” button on the function menu. The following screen will appear. Please click “Next” to continue.

Step 1: Set up new Password

User can change the password and then click “Next” to continue.



Step 2: Choose time zone

Select the time zone from the drop down list. Please click “Next” to continue.

Step 3: Set LAN connection and DHCP server

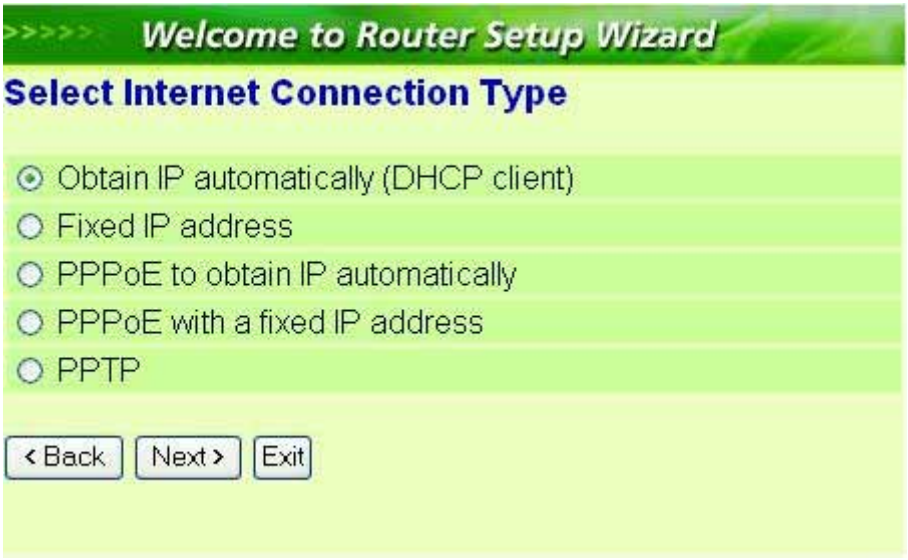
Set user’s IP address and mask. The default IP is 192.168.1.1. If user likes to enable DHCP, please click “Enabled”. DHCP enabled is able to automatically assign IP addresses. Please assign the range of IP addresses in the fields of “Range start” and “Range end”. Please click “Next” to continue.

Step 4: Set Internet connection

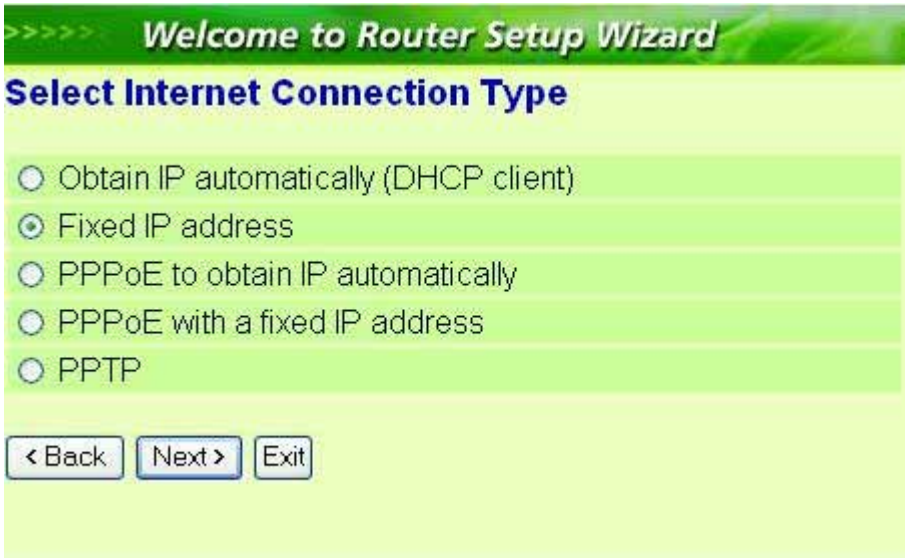
Select how the router will set up the Internet connection: Obtained IP automatically; Fixed IP address; PPPoE to obtain IP automatically; PPPoE with a fixed IP address; PPTP.

Obtain IP automatically (DHCP client):

If user has enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.



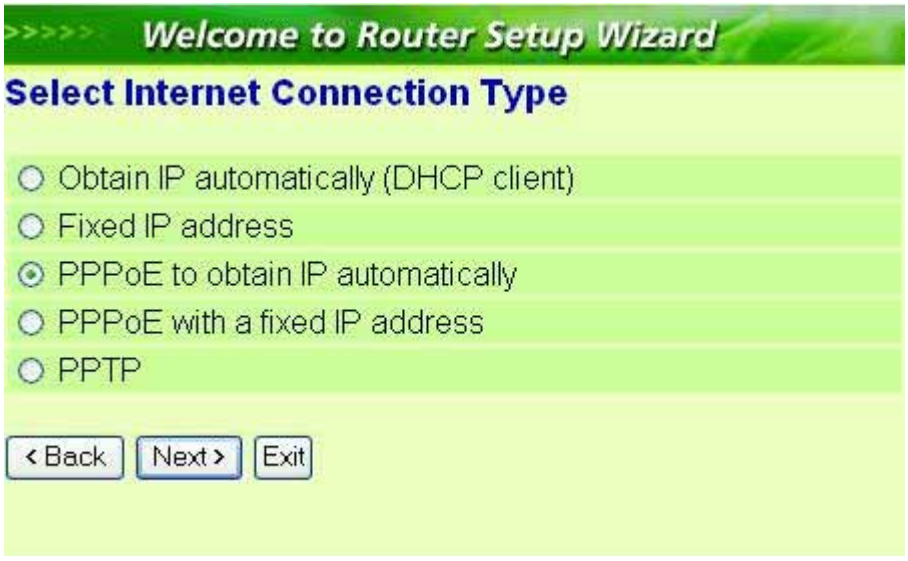
Fixed IP Address:



If the Internet Service Providers assign a fixed IP address, choose this option and enter the assigned IP address, subnet mask, gateway IP and DNS IP addresses for your Broadband Router.

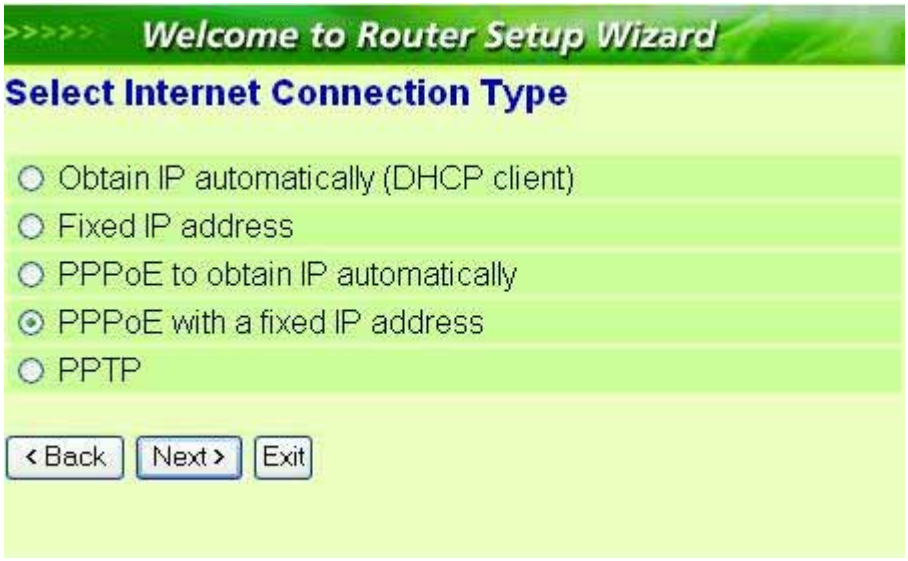
PPPoE to obtain IP automatically:

If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password and User Name, and then the ISP uses PPPoE. Choose this option and enter the required information.



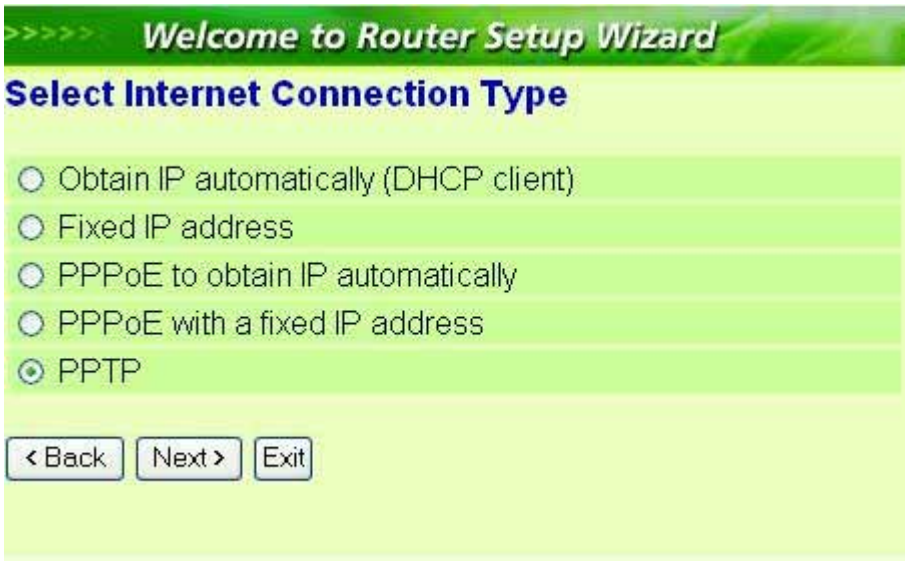
PPPoE with a fixed IP address:

If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password, User Name and a Fixed IP Address, choose this option and enter the required information.



PPTP:

If connected to the Internet using a (PPTP) xDSL Modem, enter the your IP Address, Subnet Mask, Gateway, Server IP, PPTP Account and PPTP Password, Your Subnet Mask required by your ISP in the appropriate fields. If your ISP has provided you with a Connection ID, enter it in the Connection ID field, otherwise, leave it zero.



Step 5: Set Wireless LAN connection

Click “Enable” to enable wireless LAN. If user enables the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.

Step 6: Restart

The Setup wizard is now completed. The new settings will be effective after the Wireless router restarted. Please click “Restart” to reboot the router. If user does not want to make any changes, please click “Exit” to quit without any changes. User also can go back to modify the setting by clicking “Back”.

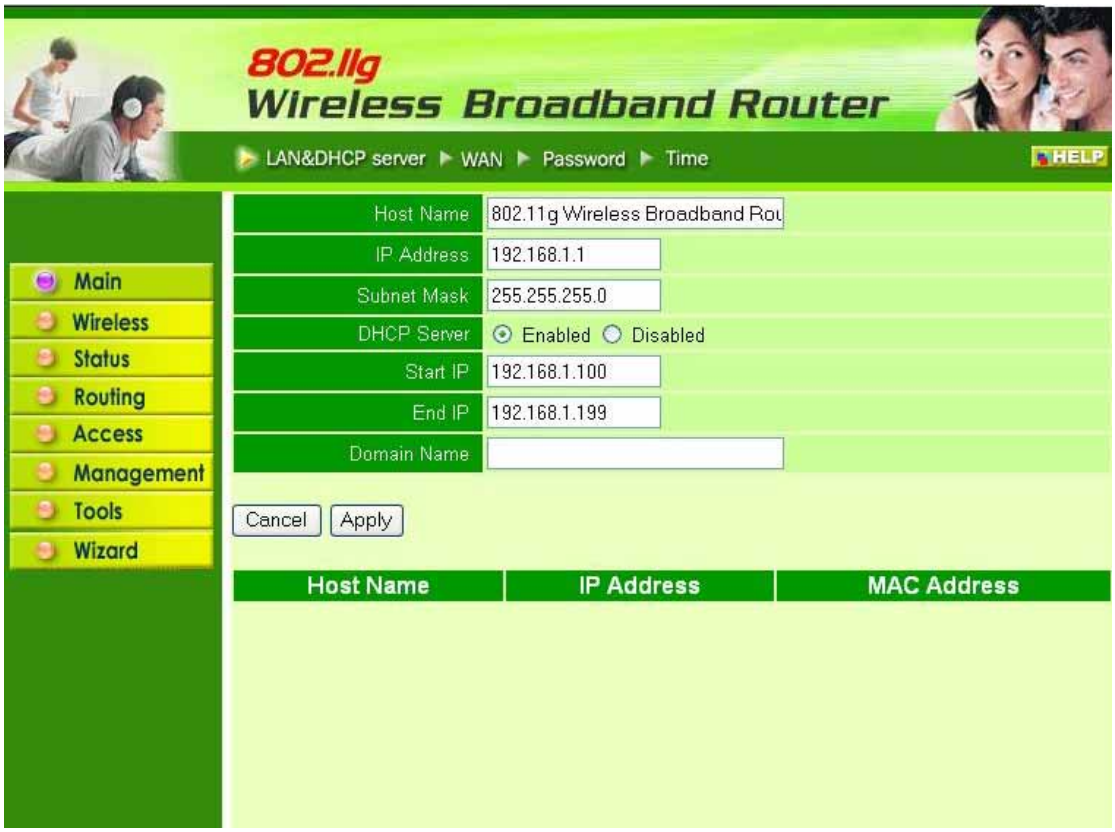
Advance Setup

2.1 LAN Setting

The screen enables user to configure the LAN & DHCP Server, set WAN parameters, create Administrator and User passwords, and set the local time, time zone, and dynamic DNS.

2.1.1 LAN & DHCP Server

This page leads to set LAN and DHCP properties, such as the host name, IP address, subnet mask, and domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.



Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is "AP-Router."

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default subnet mask is 255.255.255.0.

DHCP Server: Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default.

All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

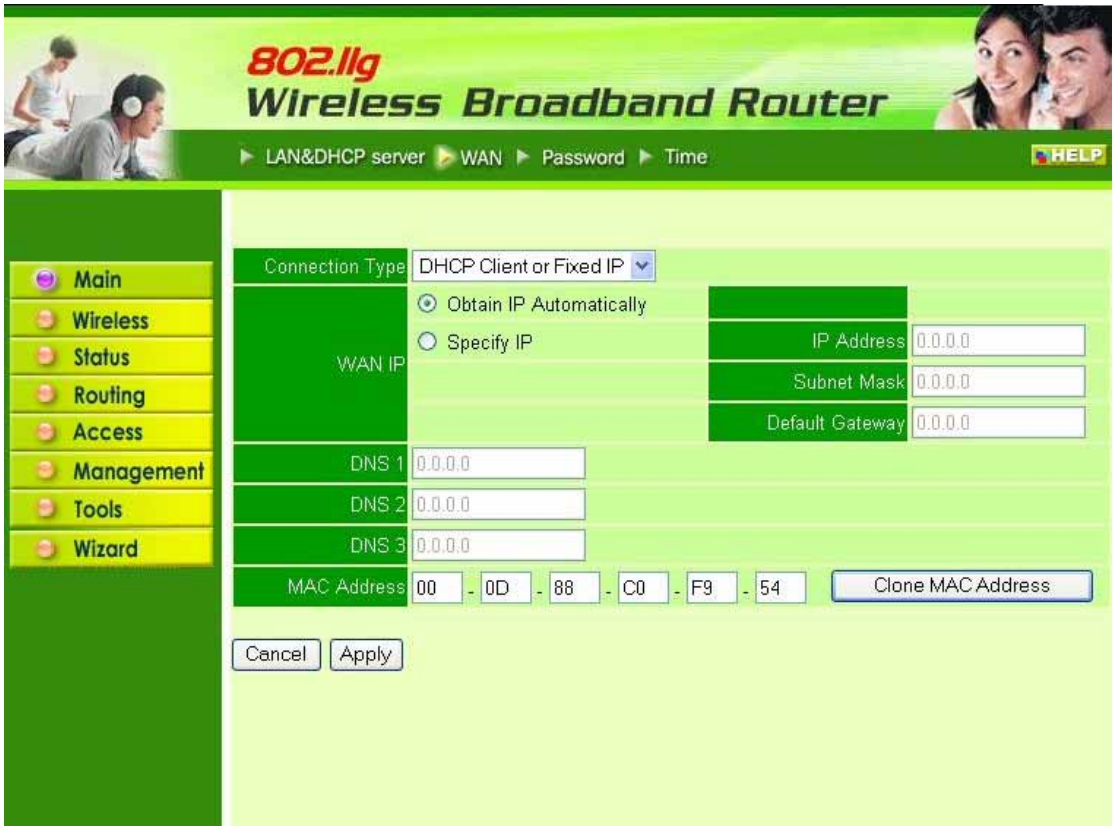
Start IP: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

End IP: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

Domain Name: Type the local domain name of the network in the text box. This item is optional.

2.1.2 WAN

This screen enables user to set up the router WAN connection, specify the IP address for the WAN, add DNS numbers, and enter the MAC address.



Connection Type: Select the connection type, either DHCP client, Fixed IP or PPPoE from the drop-down list.

WAN IP: Select whether user wants to specify an IP address manually, or want DHCP to obtain an IP address automatically. When Specify IP is selected, type the IP address, subnet mask, and default gateway in the text boxes. User's ISP will provide with this information.

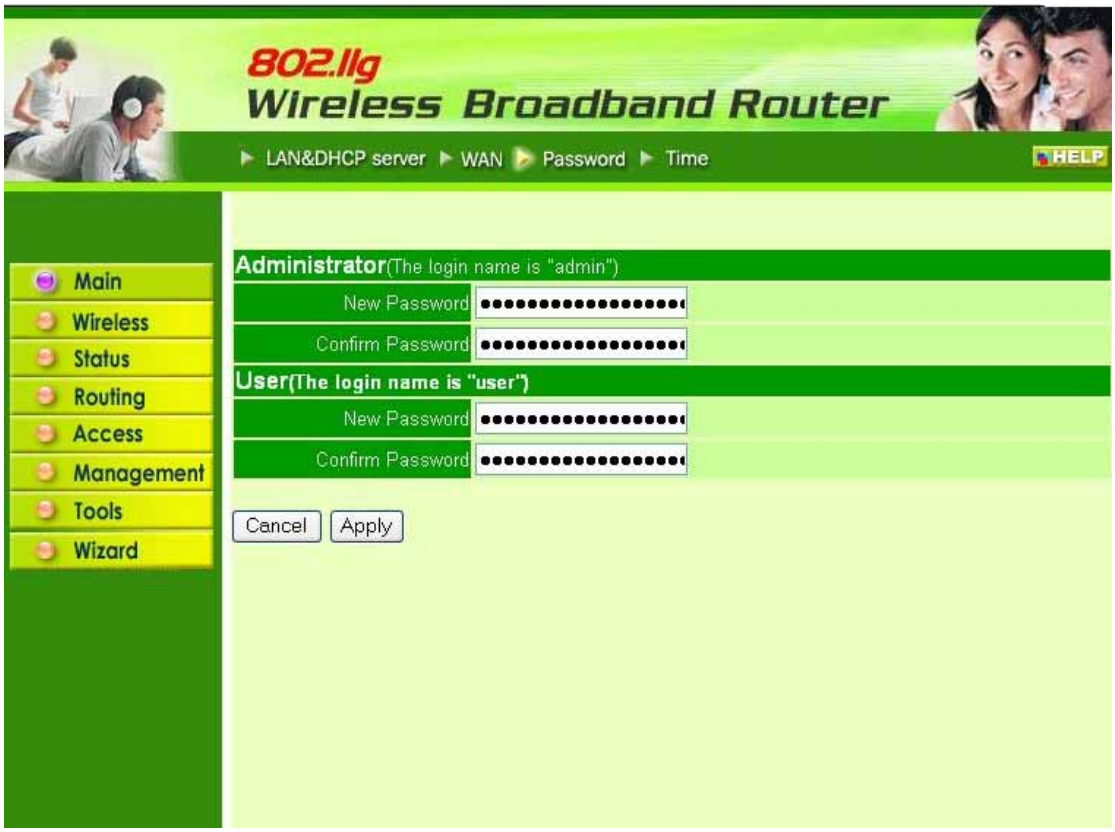
DNS 1/2/3: Type up to three DNS numbers in the text boxes. User's ISP will provide with this information.

MAC Address: If required by user's ISP, type the MAC address of the router WAN interface in this field.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. User's ISP will provide with this information.

2.1.3 Password

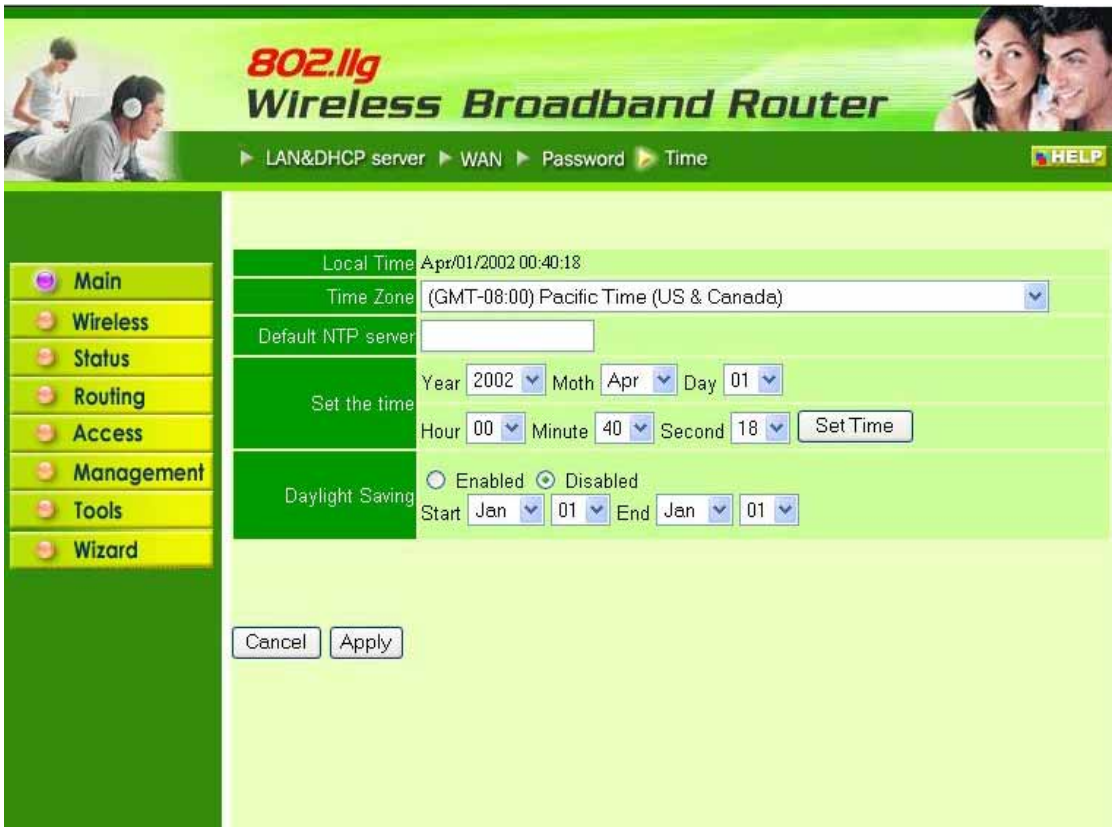
This screen enables user to set administrative and user passwords. These passwords are used to gain access to the router interface.



Administrator: Type the password the Administrator will use to log in to the system. The password must be typed again for confirmation.

2.1.4 Time

This screen enables user to set the time and date for the router's real-time clock, select properly time zone, and enable or disable daylight saving.



Local Time: Displays the local time and date.

Time Zone: Select the time zone from the drop-down list.

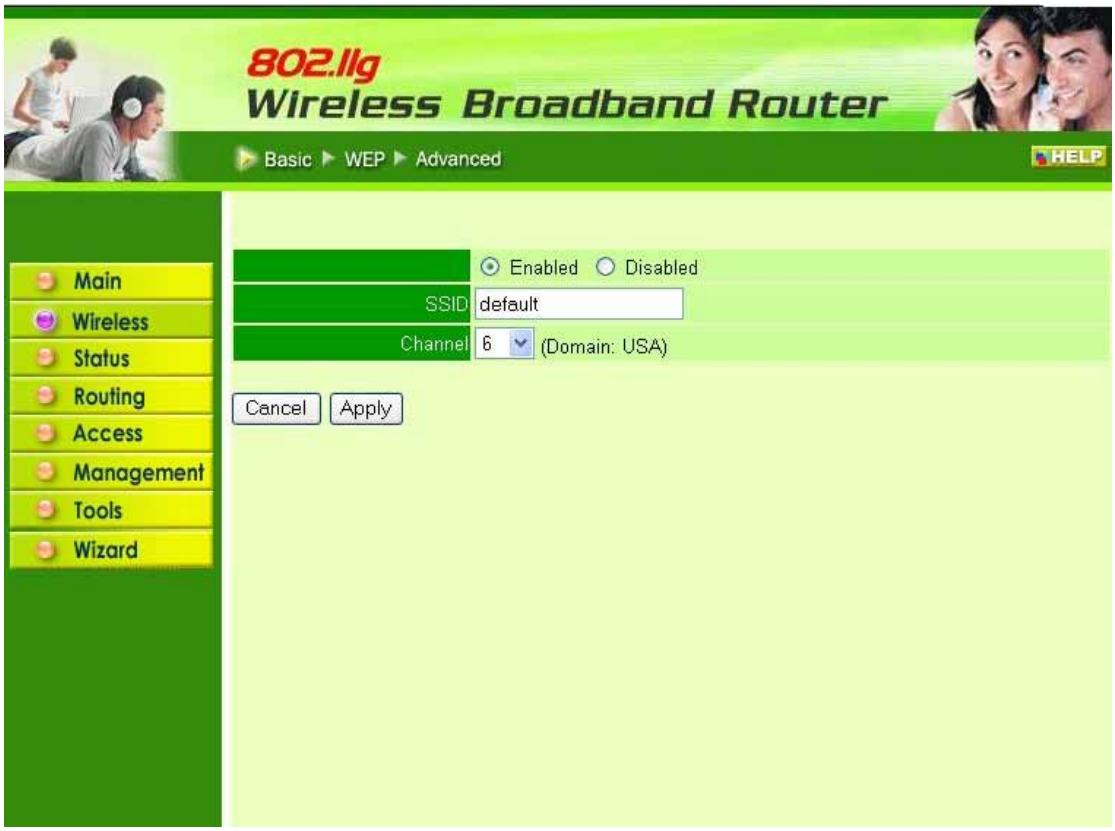
Daylight Saving: Enables user to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

2.2 Wireless

This section enables user to set wireless communications parameters for the router's wireless LAN feature.

2.2.1 Basic

This page allow user to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.



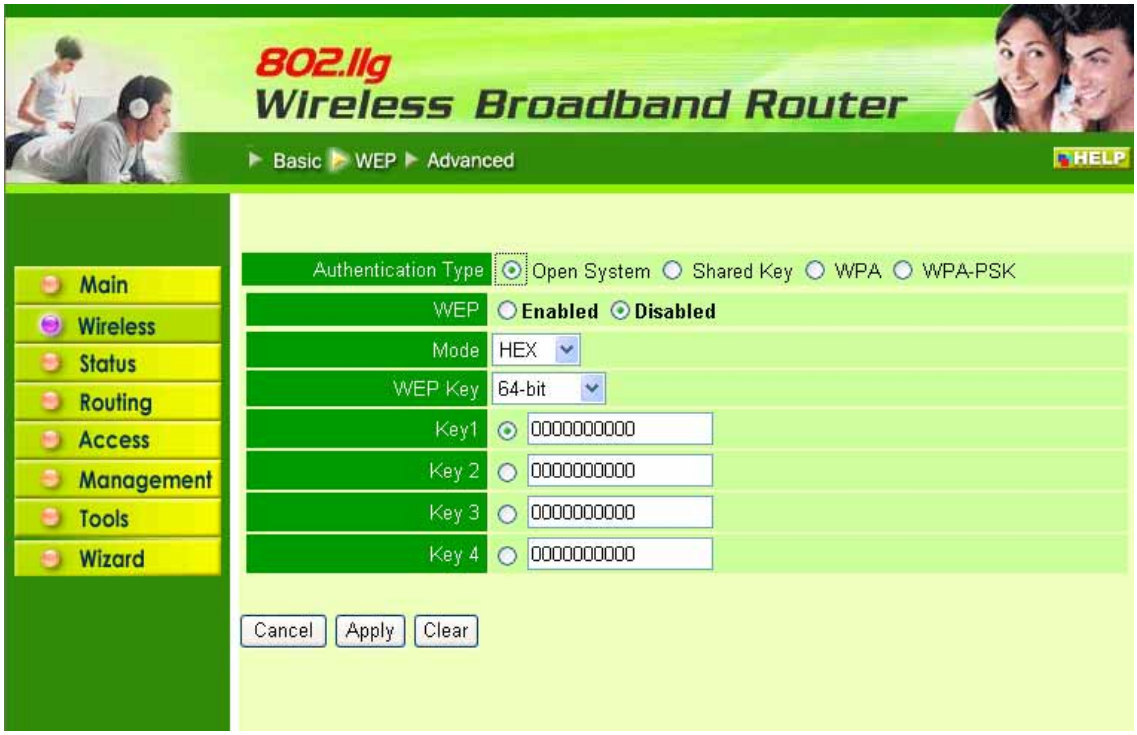
Enable/Disable: Enables and disables wireless LAN via the router.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the router.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

2.2.2 Authentication

This screen enables user to set authentication type for secure wireless communications. Open System allows public access to the router via wireless communications. Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key. This router also supports WPA and WPA-PSK.



Authentication Type: The authentication type default is set to open system. There are three options: Open System; Shared Key, WPA and WPA-PKS.

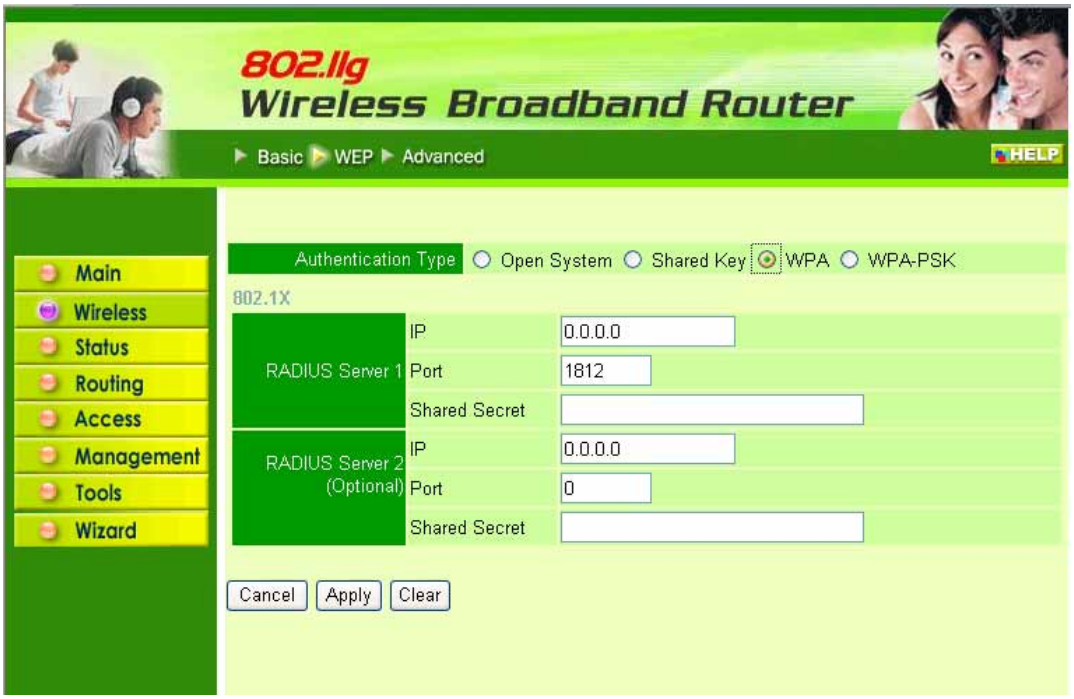
WEP: Enable or Disabled. This is to make WEP enabled or disabled.

Mode: Select the key mode in ASCII or HEX

WEP Key: Select the level of encryption from the drop-down list. The router supports, 64- and 128-bit encryption.

Key 1 ~ Key 4: Enables user to create an encryption scheme for Wireless LAN transmissions. Manually enter a set of values for each key. Select a key to use by clicking the radio button next to the key. Click **"Clear"** to erase key values.

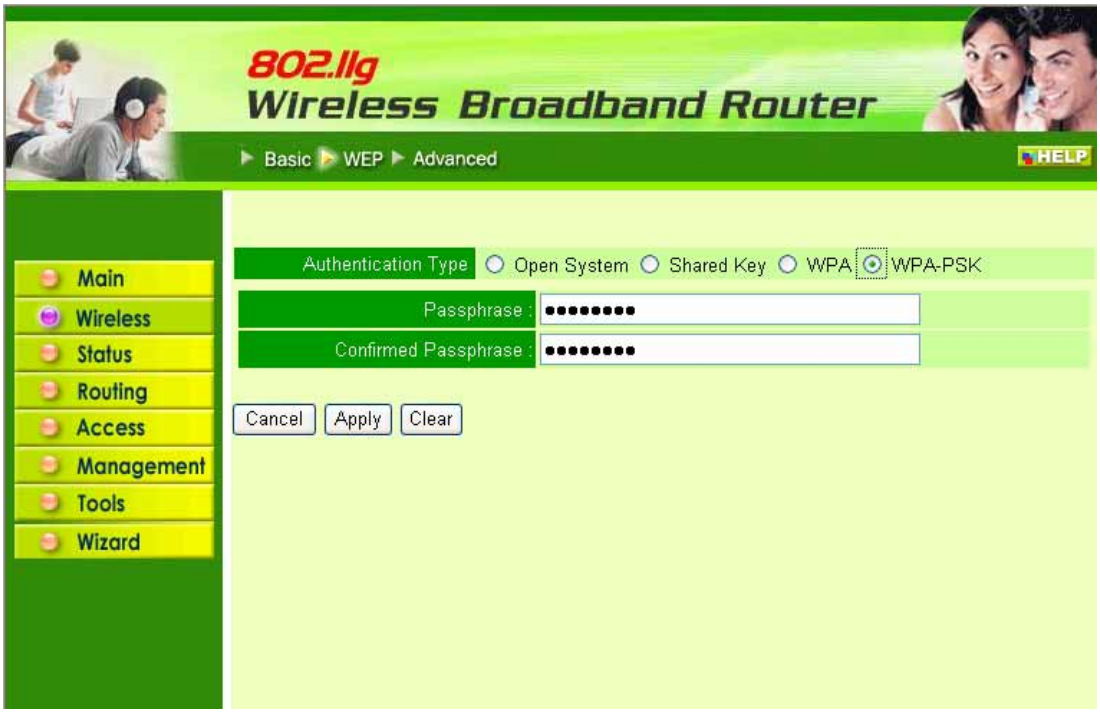
If **WPA** is selected, the below screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.



RADIUS Server:

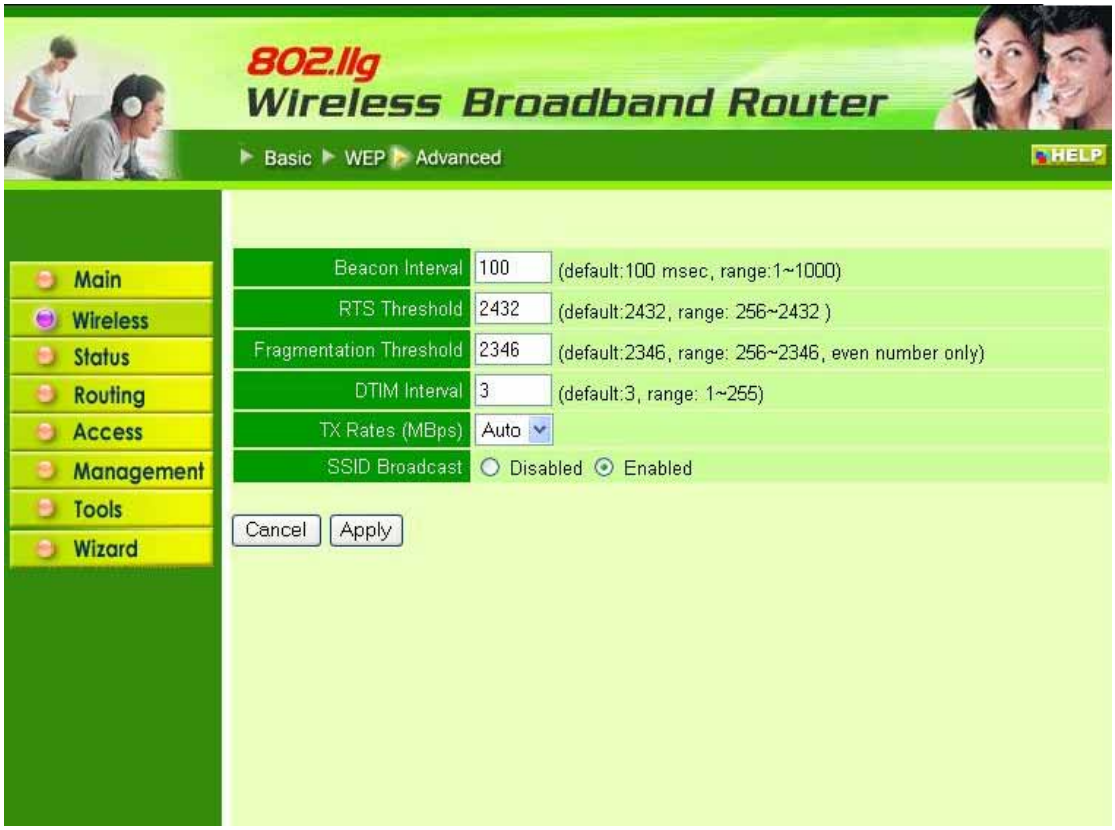
1. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server
   Enter the **Shared Secret**, which is used by the Radius Server.
2. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.

If **WPA-PSK** is selected, please set the PSK key in the pass phrase field. The pass phrase should be 8 characters at least.



2.2.3 Advanced

This screen enables user to configure advanced wireless functions.



Beacon Interval: Type the beacon interval in the text box. User can specify a value from 1 to 1000. The default beacon interval is 100.

RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2432 until data flow is normalized.

Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 256 and 2432 until packet transfer rates are minimized. (NOTE: set this fragmentation threshold value may diminish system performance.)

DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. User can specify a value between 1 and 65535. The default value is 3.

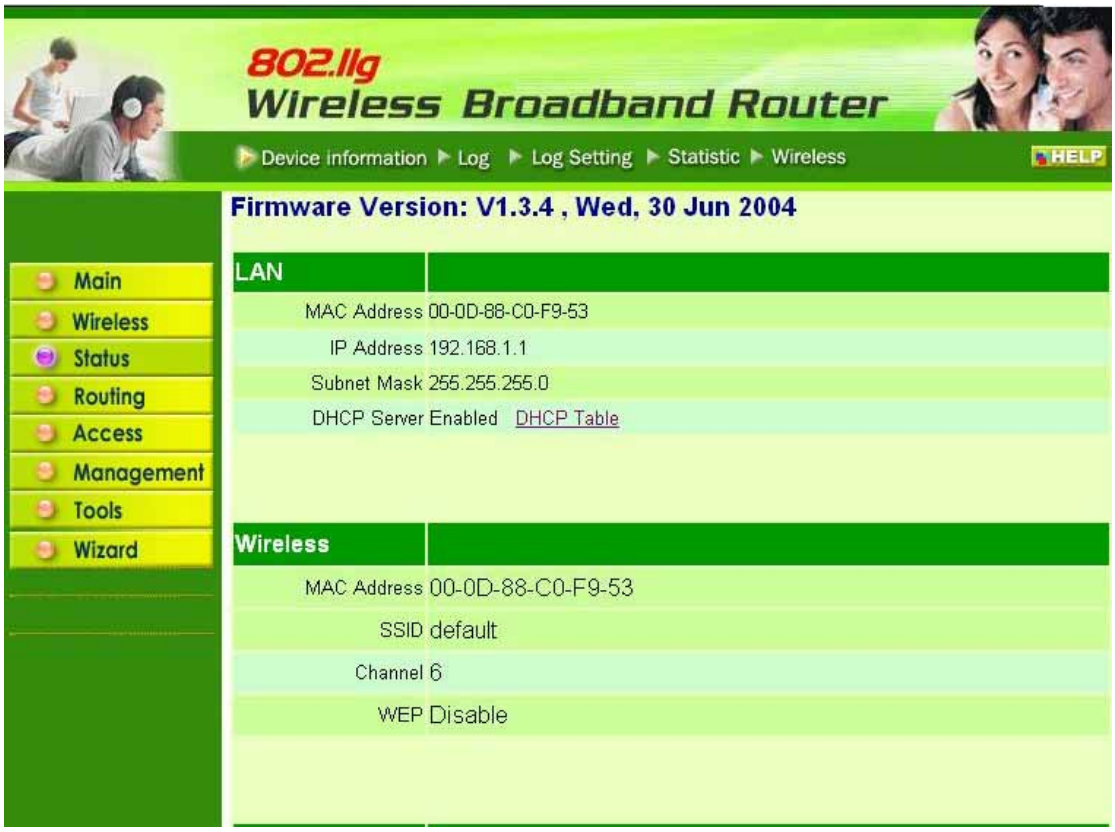
TX Rates (Mbps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

2.3 Status

This selection enables user to view the status of the router LAN, WAN connections, and view logs and statistics pertaining to connections and packet transfers.

2.3.1 Device Information

This screen enables user to view the router LAN, Wireless and WAN configuration.



Firmware Version: Displays the latest build of the router firmware interface. After updating the firmware in Tools - Firmware, check this to ensure that the firmware was successfully updated.

LAN: This field displays the router's LAN interface MAC address, IP address, subnet mask, and DHCP server status. Click “DHCP Table” to view a list of client stations currently connected to the router LAN interface.

Wireless: Displays the router's wireless connection information, including the router's wireless interface MAC address, the connection status, the SSID status, which channel is being used, and whether WEP is enabled or not.

WAN: This field displays the router's WAN interface MAC address, DHCP client status, IP address, subnet mask, default gateway, and DNS.

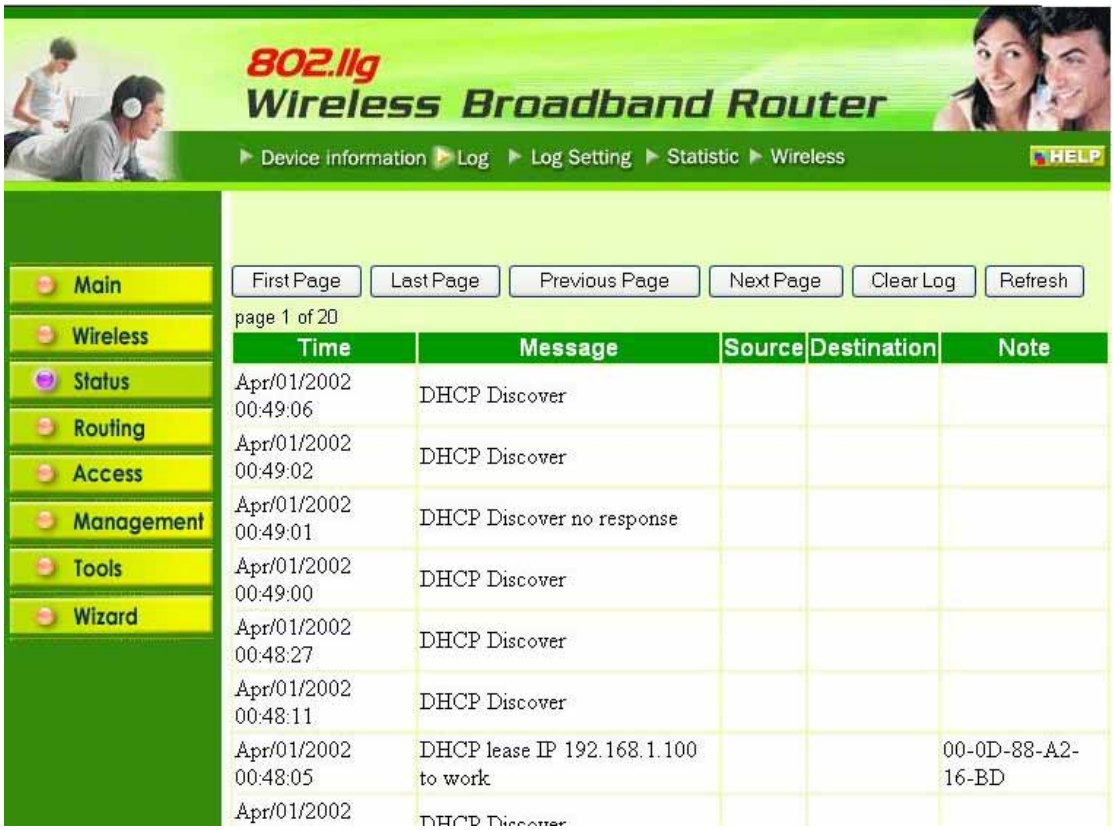
Click “DHCP Release” to release all IP addresses assigned to client stations connected to the WAN via the router. Click “DHCP Renew” to reassign IP addresses to client stations connected to the WAN.

2.3.2 Log

This screen enables user to view a running log of router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:

Click “First Page” to view the first page of the log

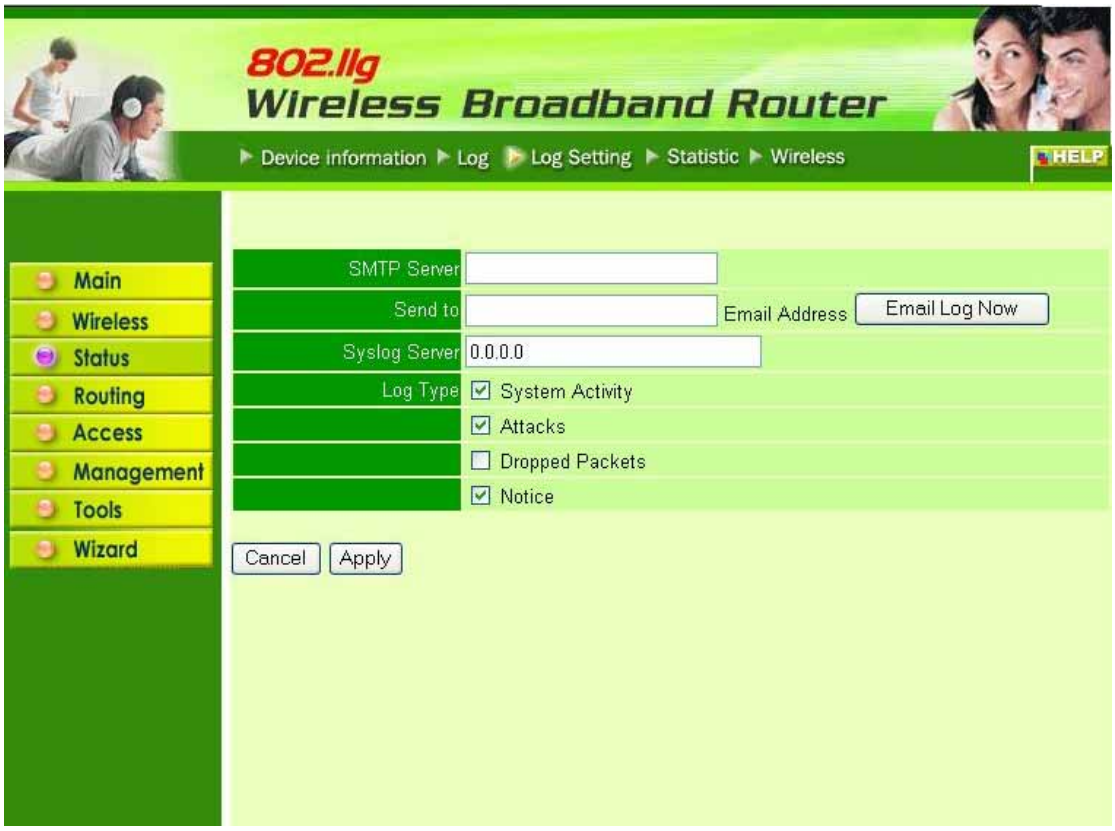
Click “Last Page” to view the final page of the log
Click “Previous Page” to view the page just before the current page
Click “Next Page” to view the page just after the current page
Click “Clear Log” to delete the contents of the log and begin a new log
Click “Refresh” to renew log statistics



Time: Displays the time and date that the log entry was created.
Message: Displays summary information about the log entry.
Source: Displays the source of the communication.
Destination: Displays the destination of the communication.
Note: Displays the IP address of the communication

2.3.3 Log Setting

This screen enables user to set router logging parameters.



SMTP Server: Type the SMTP server address for the email that the log will be sent to in the next field.

Send to: Type an email address for the log to be sent to. Click “Email Log Now” to immediately send the current log.

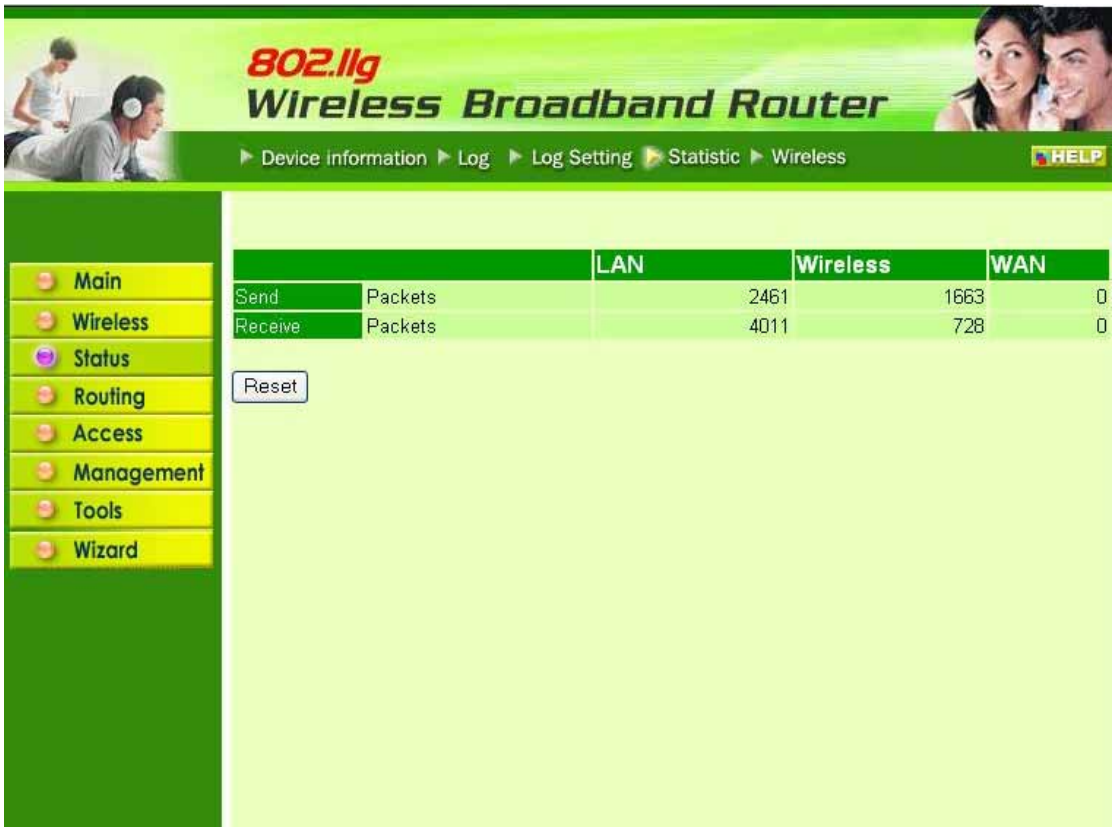
Syslog Server: Type the IP address of the Syslog Server if user wants the router to listen and receive incoming Syslog messages.

Log Type: Enables user to select what items will be included in the log:

- **System Activity:** Displays information related to router operation.
- **Debug Information:** Displays information related to errors and system malfunction.
- **Attacks:** Displays information about any malicious activity on the network.
- **Dropped Packets:** Displays information about packets that have not been transferred successfully.
- **Notice:** Displays important notices by the system administrator.

2.3.4 Statistic

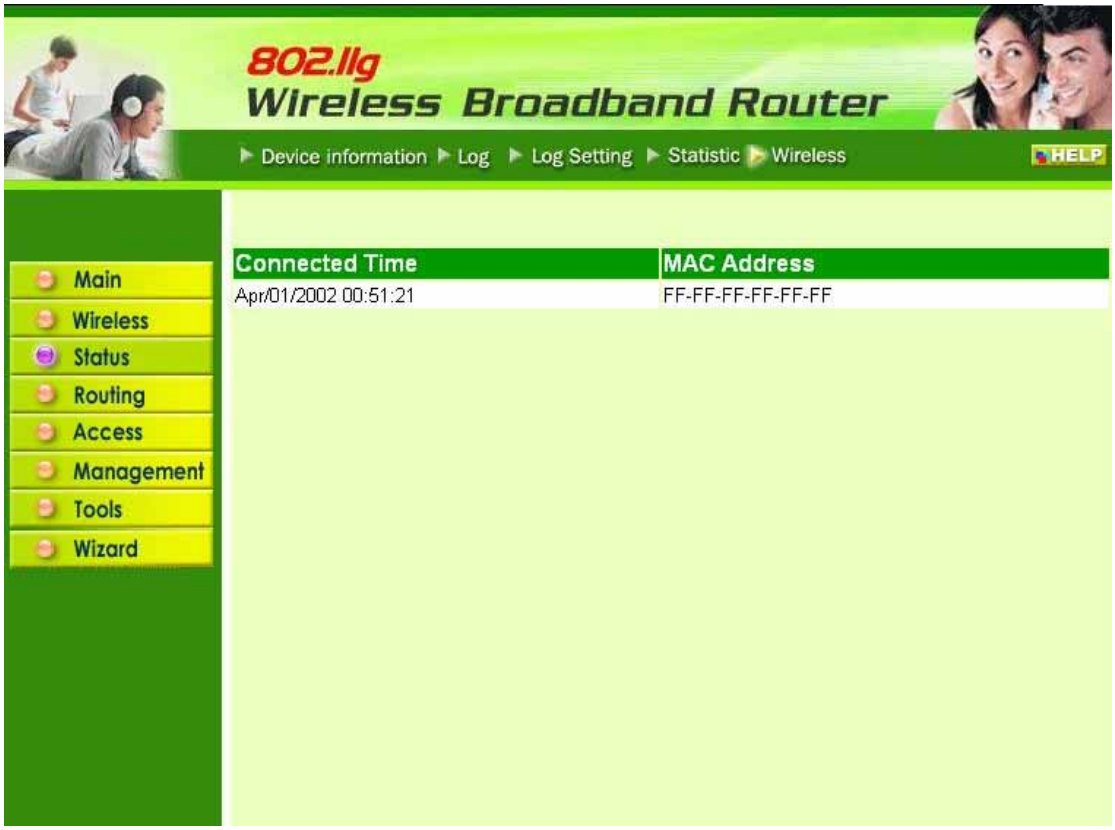
This screen displays a table that shows the rate of packet transmission via the router LAN and WAN ports (in bytes per second).



Click “Reset” to erase all statistics and begin logging statistics again.

2.3.5 Wireless

This screen enables user to view information about wireless devices that are connected to the wireless router.



Connected Time: Displays how long the wireless device has been connected to the LAN via the router.

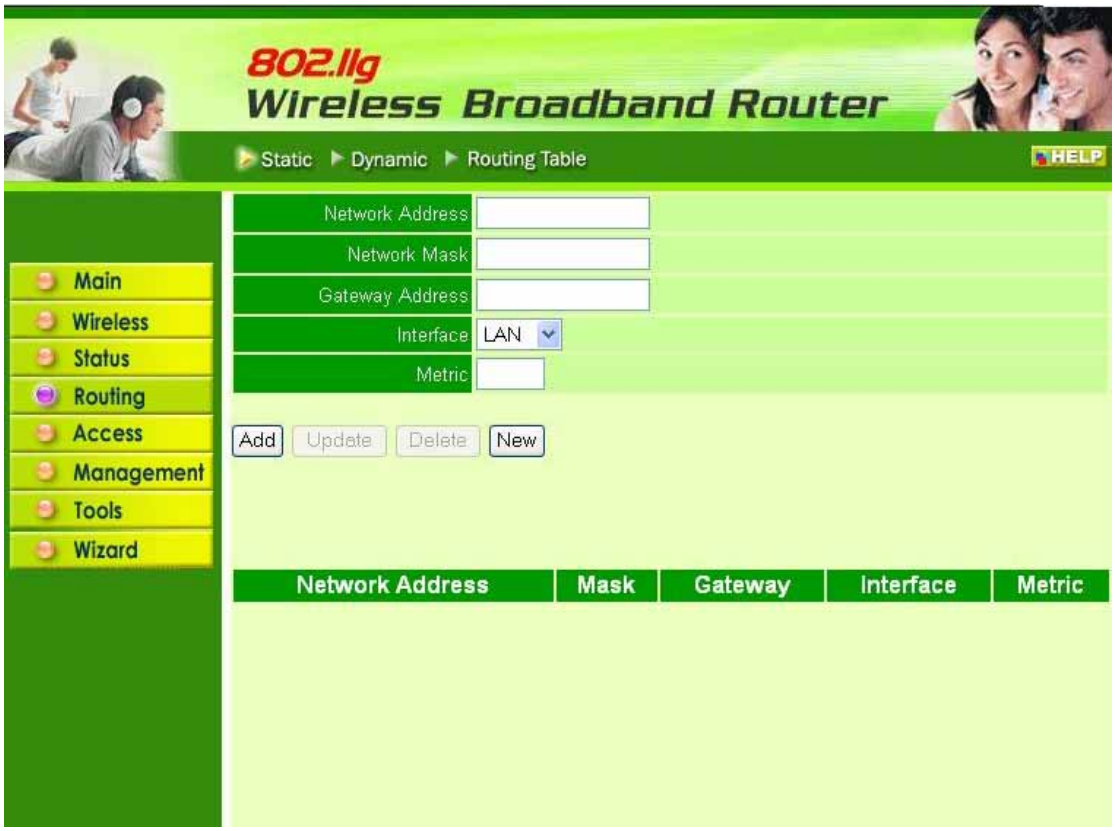
MAC Address: Displays the devices wireless LAN interface MAC address.

2.4 Routing

This selection enables user to set how the router forwards data: Static and Dynamic. Routing Table enables user to view the information created by the router that displays the network interconnection topology.

2.4.1 Static

It enables user to set parameters by which the router forwards data to its destination if user's network has a static IP address.



Network Address: Type the static IP address user's network uses to access the Internet. User's ISP or network administrator provides user with this information.

Network Mask: Type the network (subnet) mask for user's network. If user does not type a value here, the network mask defaults to 255.255.255.255. User's ISP or network administrator provides user with this information.

Gateway Address: Type the gateway address for network. User's ISP or network administrator provides user with this information.

Interface: Select an interface, WAN or LAN, to connect to the Internet.

Metric: Select which metric that user want to apply to this configuration.

Add: Click to add the configuration to the static IP address table at the bottom of the page.

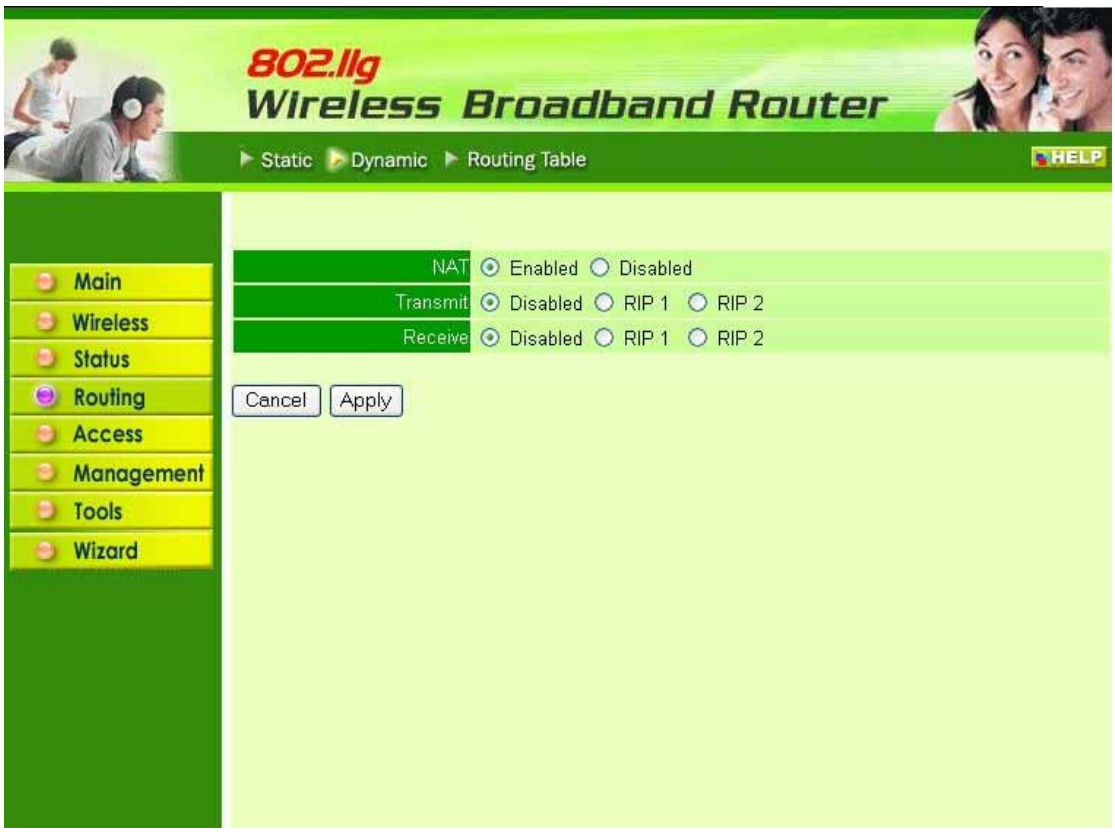
Update: Select one of the entries in the static IP address table at the bottom of the page and, after changing parameters, click "Update" to confirm the changes.

Delete: Select one of the entries in the static IP address table at the bottom of the page and click “Delete” to remove the entry.

New: Click “New” to clear the text boxes and add required information to create a new entry.

2.4.2 Dynamic

This screen enables user to set NAT parameters.



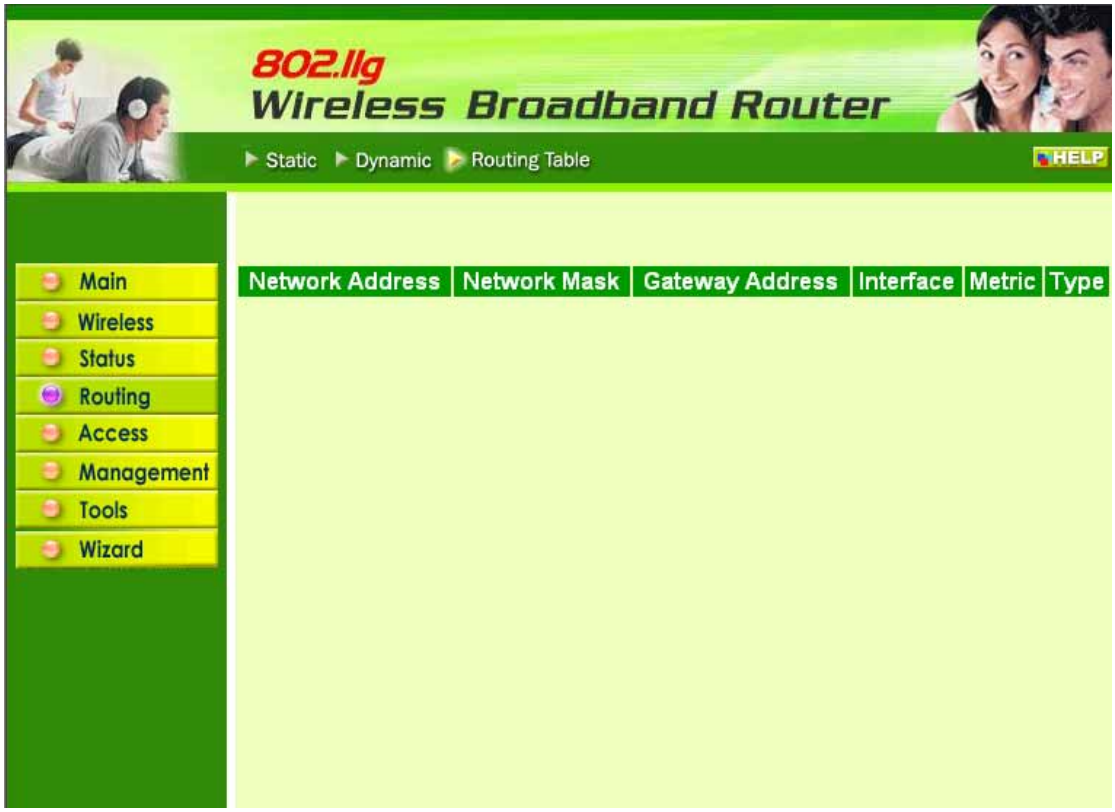
NAT: Click the radio buttons to enable or disable NAT.

Transmit: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.

Receive: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.

2.4.3 Routing Table

This screen enables user to view the routing table for the router. The routing table is a database created by the router that displays the network interconnection topology.



Network Address: Displays the network IP address of the connected node.

Network Mask: Displays the network (subnet) mask of the connected node.

Gateway Address: Displays the gateway address of the connected node.

Interface: Displays whether the node is connected via a WAN or LAN.

Metric: Displays the metric of the connected node.

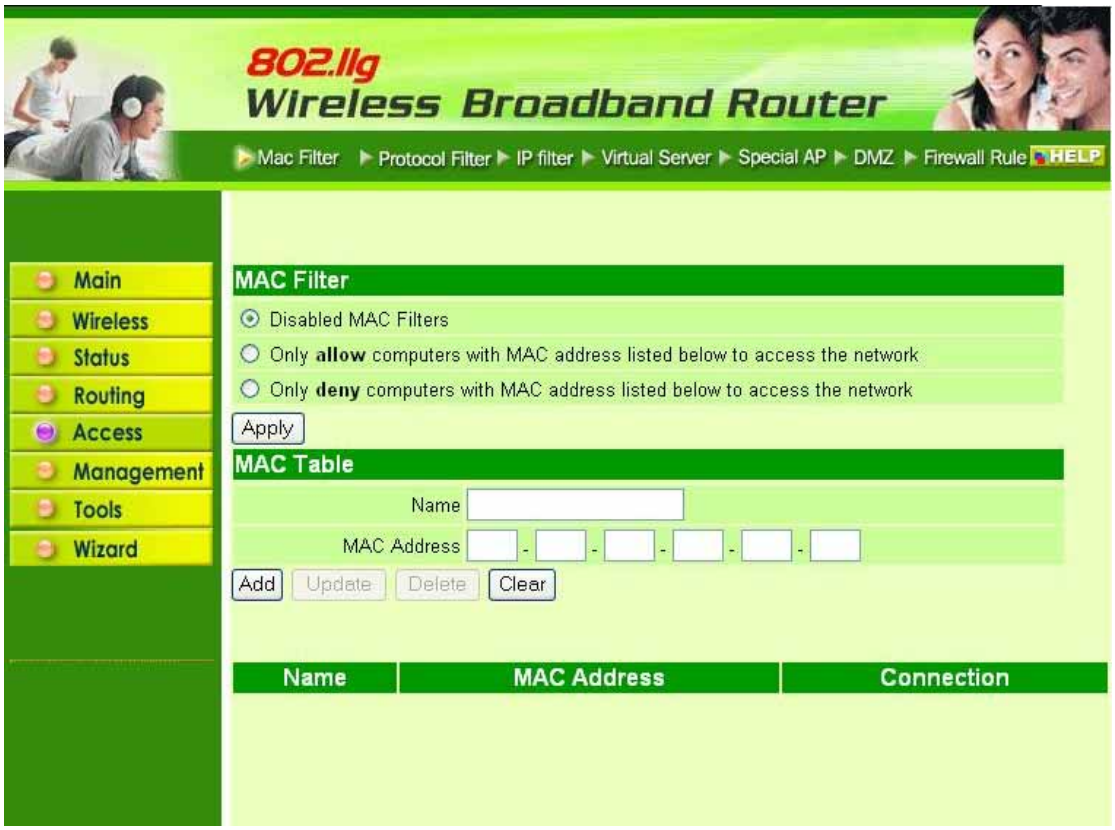
Type: Displays whether the node has a static or dynamic IP address

2.5 Access

This page enables user to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

2.5.1 MAC Filters

Enables user to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to “Disabled” to disable the MAC filter.



Disable: Once the function of MAC filter is disabled, those listed in the MAC Table are allowed Internet access.

Enable: All users are allowed Internet access except those users in the MAC Table are denied Internet access.

MAC Table: Use this section to create a user profile which Internet access is denied or allowed. The user profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which user can edit.)

Name: Type the name of the user to be permitted/denied access.

MAC Address: Type the MAC address of the user's network interface.

Add: Click to add the user to the list at the bottom of the page.

Update: Click to update information for the user, if user has changed any of the fields.

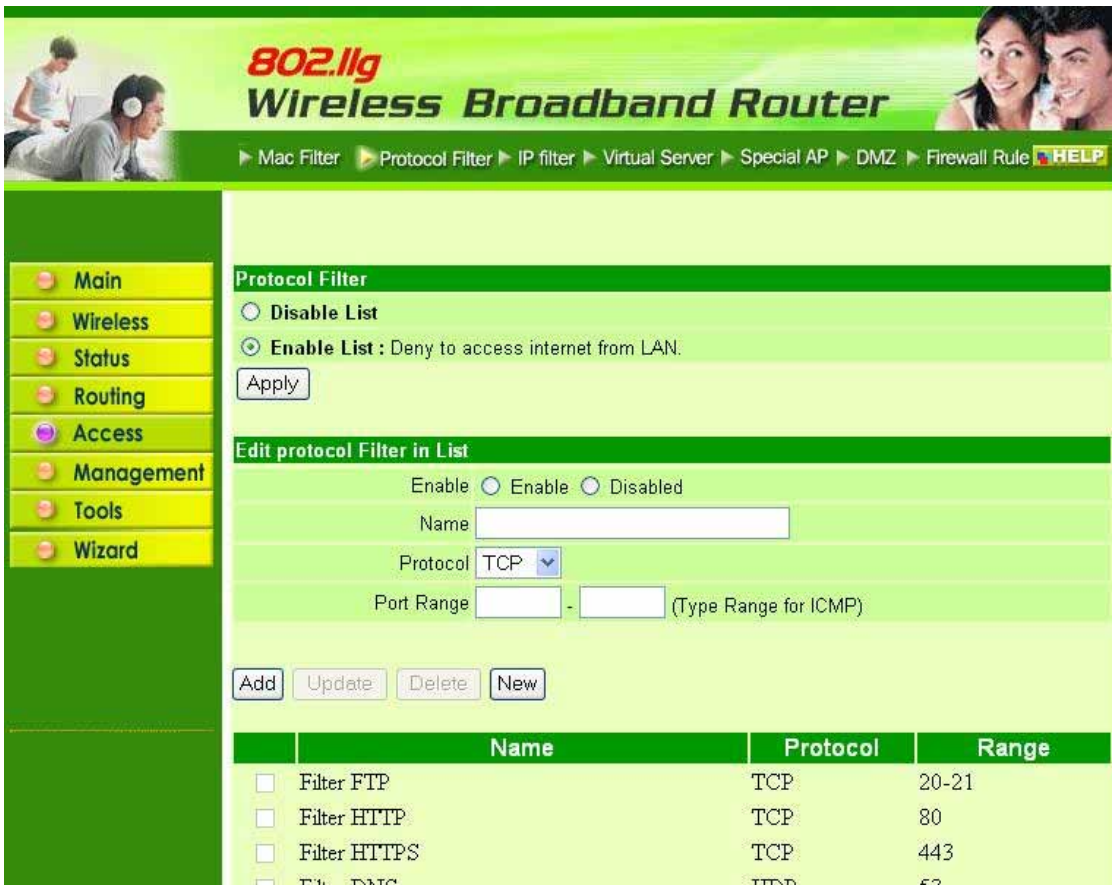
Delete: Select a user from the table at the bottom of the list and click “Delete” to remove the user profile.

New: Click “New” to erase all fields and enter new information.

2.5.2 Protocol Filter

This screen enables user to allow and deny access based upon a communications protocol list the user creates. The protocol filter profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit:



2.5.3 IP Filter

This screen enables user to define a minimum and maximum IP address range filter; all IP addresses falling in the range are not allowed Internet access. The IP filter profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which user can edit.)

Enable: Click to enable or disable the IP address filter.

Range Start: Type the minimum address for the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.

Range End: Type the minimum address for the IP range. IP addresses falling between this value and the Range Start are not allowed to access the Internet.

Add: Click to add the IP range to the table at the bottom of the screen.

Update: Click to update information for the range if user have selected a list item and have made changes.

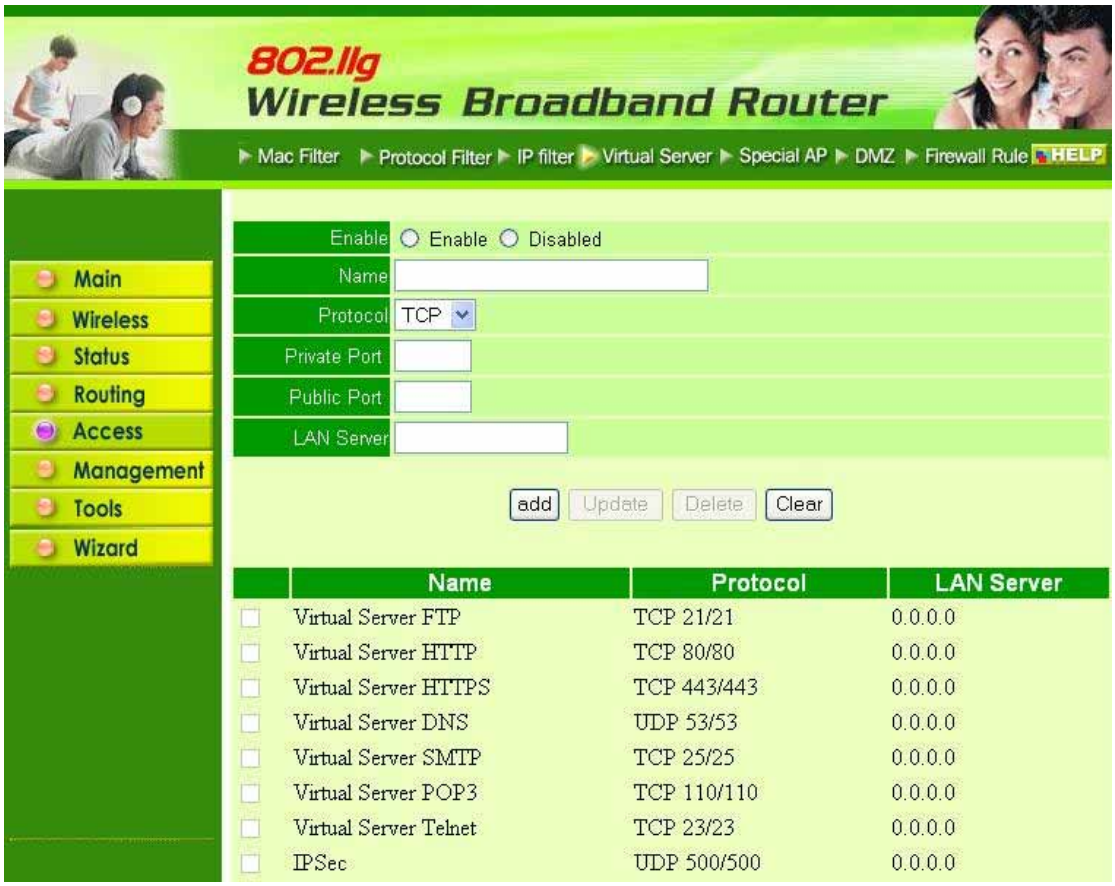
Delete: Select a list item and click Delete to remove the item from the list.

New: Click “New” to erase all fields and enter new information.

2.5.4 Virtual Server

This screen enables user to create a virtual server via the router. If the router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.



Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select a protocol (TCP or UDP) to use for the virtual server.

Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

LAN Server: Type the LAN IP address that will be assigned to the virtual server.

Add: Click to add the virtual server to the table at the bottom of the screen.

Update: Click to update information for the virtual server if user have selected a list item and have made changes.

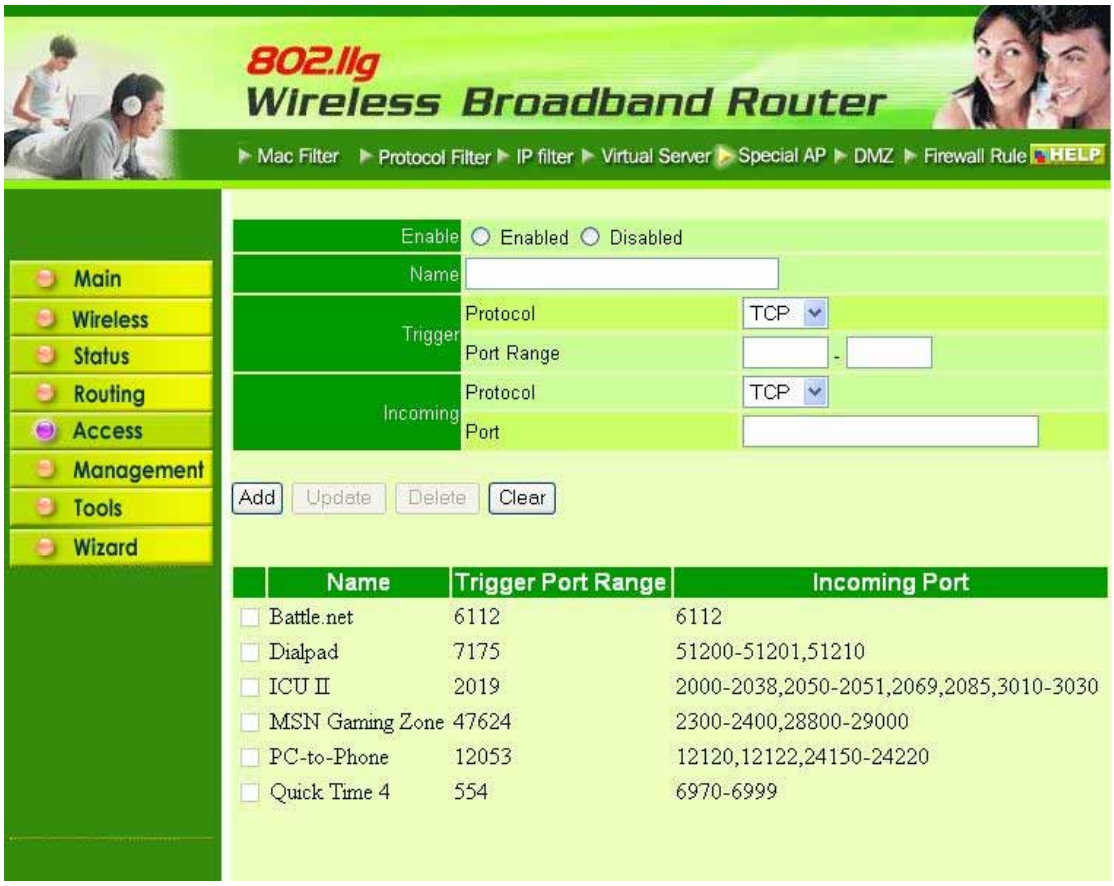
Delete: Select a list item and click “Delete” to remove the item from the list.

New: Click “New” to erase all fields and enter new information.

2.5.5 Special AP

This screen enables user to specify special applications, such as games, that require multiple connections that are inhibited by NAT. The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.



Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the router WAN connection. Click “Disabled” on a profile to prevent users from accessing the application on the WAN.

Name: Type a descriptive name for the application.

Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.

- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used to access the application.
- **Port Range:** Type the port range that can be used to access the application in the text boxes.
- **Incoming:** Defines which incoming communications users are permitted to connect with.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used by the incoming communication.
- **Port:** Type the port number that can be used for the incoming communication.

Add: Click to add the special application profile to the table at the bottom of the screen.

Update: Click to update information for the special application if user have selected a list item and have made changes.

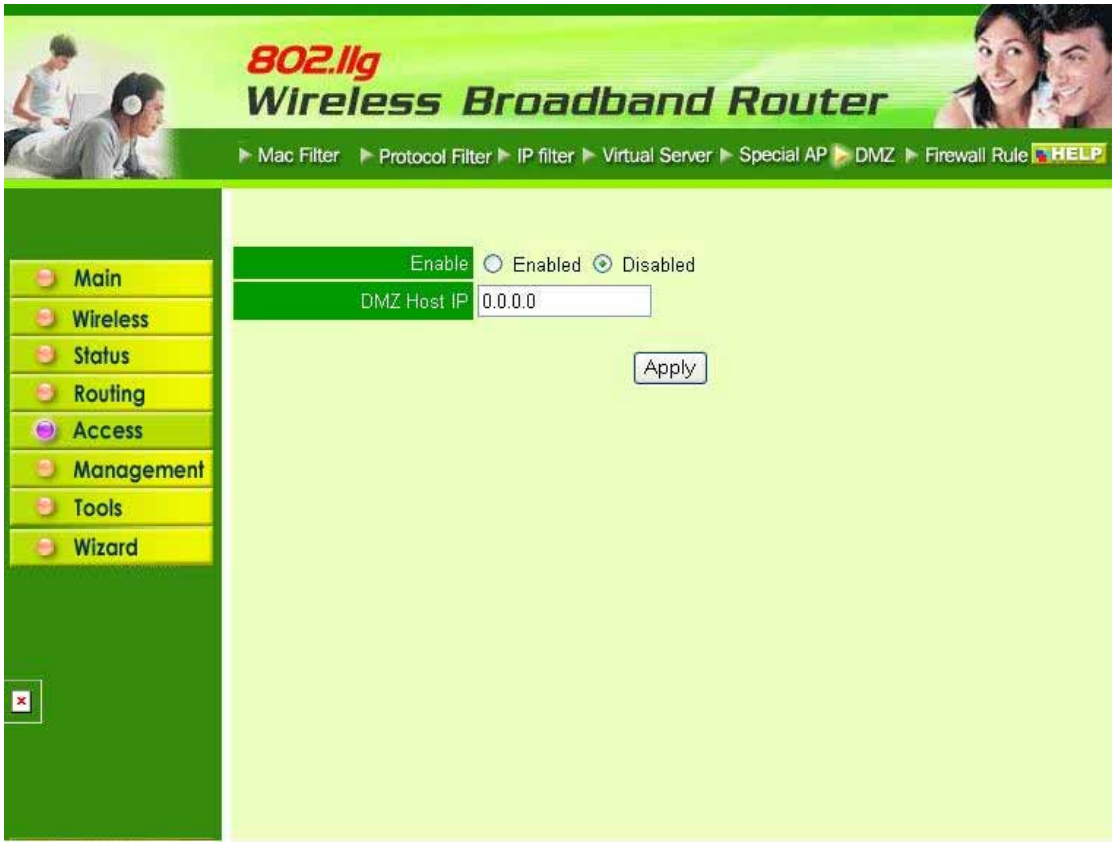
Delete: Select a list item and click Delete to remove the item from the list.

New: Click “New” to erase all fields and enter new information.

2.5.6 DMZ

This screen enables user to create a DMZ for those computers that cannot access Internet applications properly through the router and associated security settings.

Note: Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.



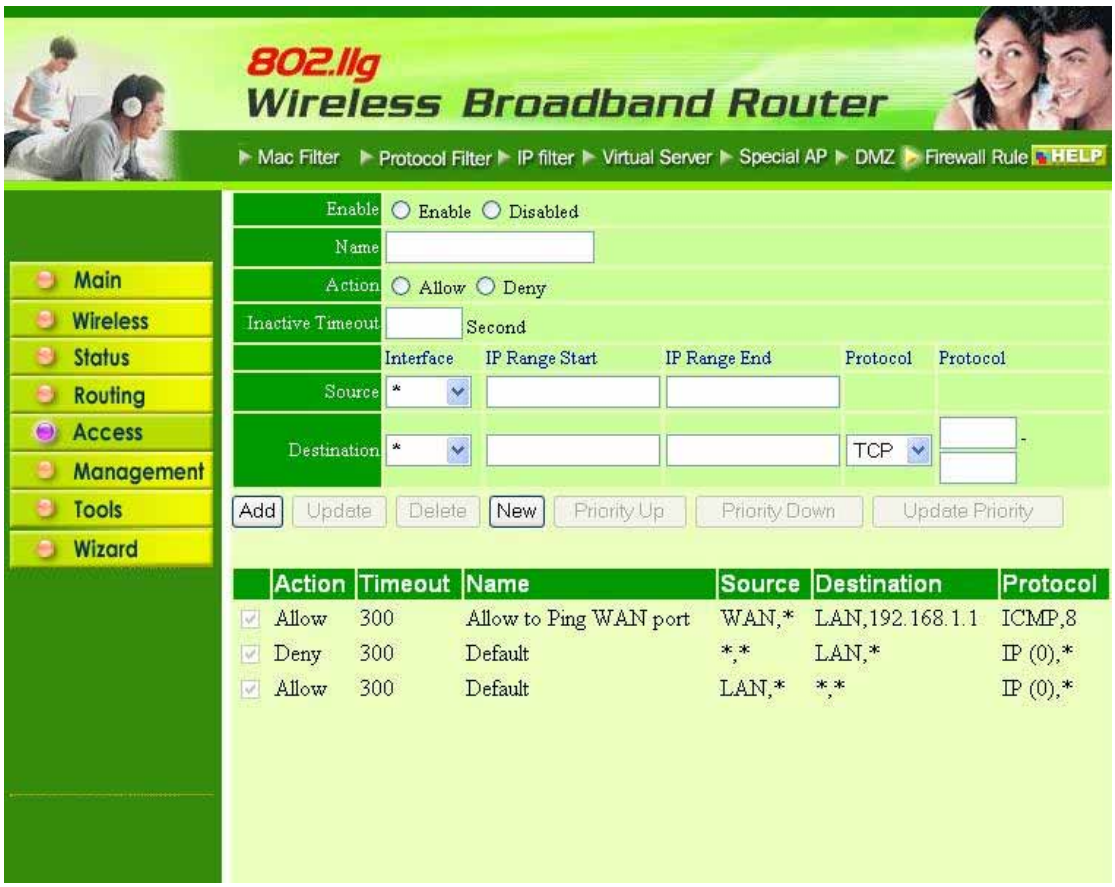
Enable: Click to enable or disable the DMZ.

DMZ Host IP: Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Apply: Click to save the settings.

2.5.7 Firewall Rule

This screen enables user to set up the firewall. The router provides basic firewall functions, by filtering all the packets that enter the router using a set of rules. The rules are in an order sequence list--the lower the rule number, the higher the priority the rule has.



Enable: Click to enable or disable the firewall rule profile.

Name: Type a descriptive name for the firewall rule profile.

Action: Select whether to allow or deny packets that conform to the rule.

Inactive Timeout: Type the number of seconds of network inactivity that elapses before the router refuses the incoming packet.

Source: Defines the source of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.

Destination: Defines the destination of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
- **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.

Update: Click to update information for the rule if user have selected a list item and have made changes.

Delete: Select a list item and click **"Delete"** to remove the item from the list.

New: Click **"New"** to erase all fields and enter new information.

Priority Up: Select a rule from the list and click **"Priority Up"** to increase the priority of the rule.

Priority Down: Select a rule from the list and click **"Priority Down"** to decrease the priority of the rule.

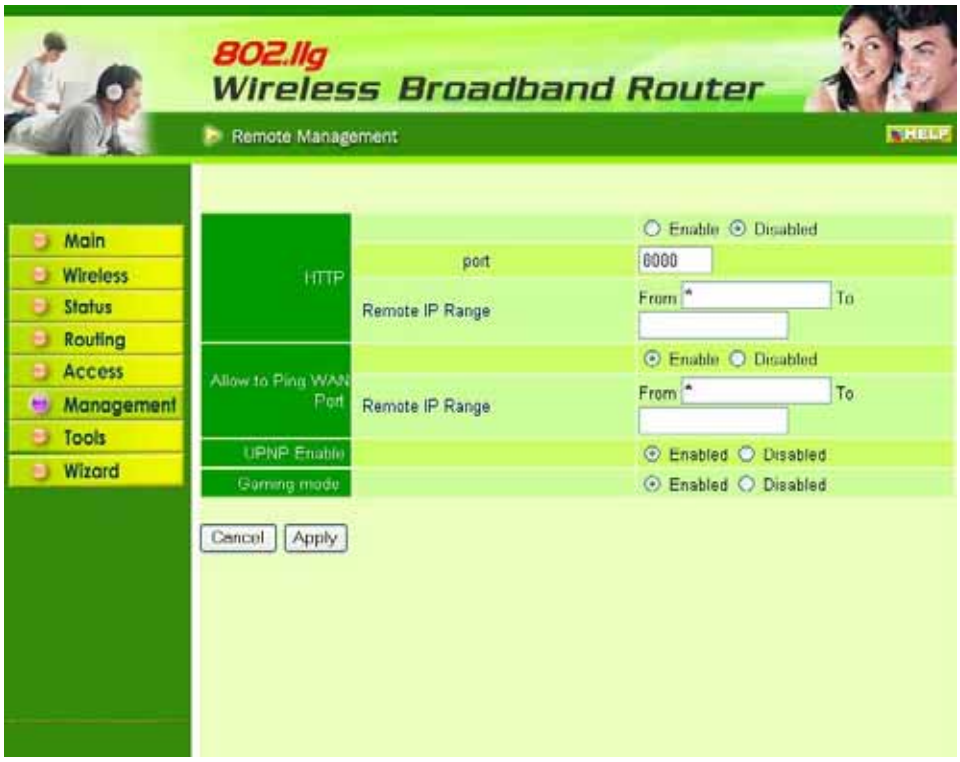
Update Priority: After increasing or decreasing the priority of a rule, click **"Update Priority"** to save the changes.

2.6 Management

Management enables user to set up Remote Management feature.

2.6.1 Remote Management

This screen enables user to set up remote management. Using remote management, the router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.



HTTP: Enables user to set up HTTP access for remote management.

Allow to Ping WAN Port: Type a range of router IP addresses that can be pinged from remote locations

UPNP: UPNP is short for Universal Plug and Play that is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The Router is an UPnP enabled router and will only work with other UPnP devices/software. If user does not want to use the UPnP functionality, selecting “Disabled” can disable it.

GAMING MODE: If user is experiencing difficulties when playing online games or even certain applications that use voice data, user may need to enable Gaming Mode for these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode be disabled.

PPTP: Enables user to set up PPTP access for remote management.

IPSec: Enables user to set up IPSec access for remote management.

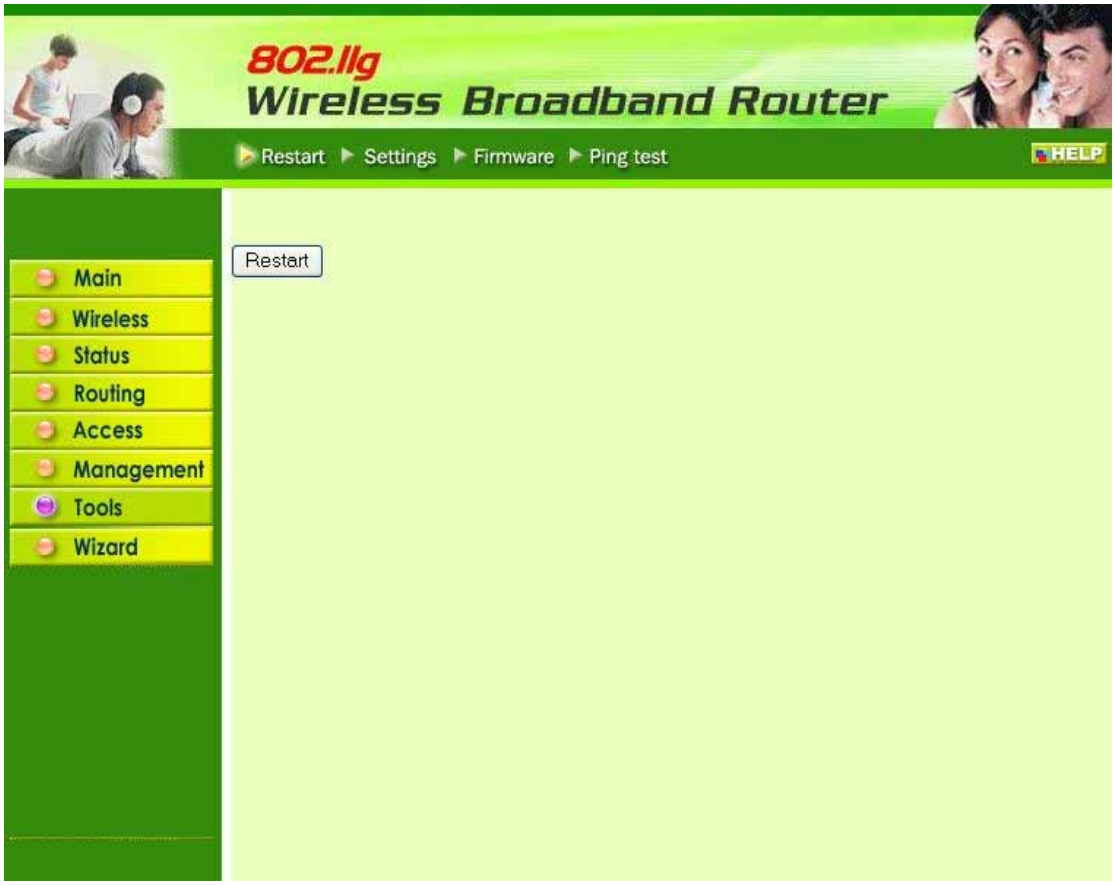
IDENT: Default is stealth. This enables user to set port 113 stealth.

2.7 Tools

This page enables user to restart the system, save and load different settings as profiles, restore factory default settings, run a setup wizard to configure router settings, upgrade the firmware, and ping remote IP addresses.

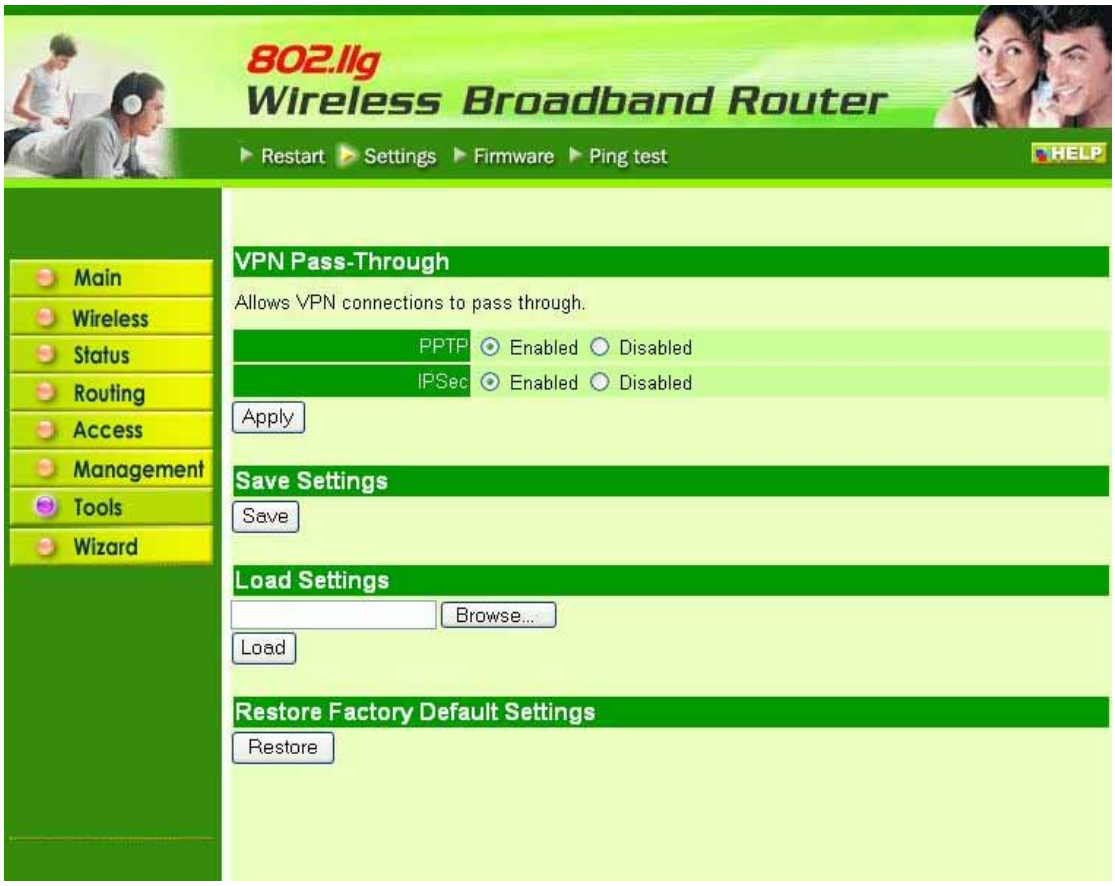
2.7.1 Reset

Click “Restart” to restart the system in the event the system is not performing correctly.



2.7.2 Settings

This screen enables user to save settings as a profile and load profiles for different circumstances. User can also load the factory default settings, and run a setup wizard to configure the router and router interface.



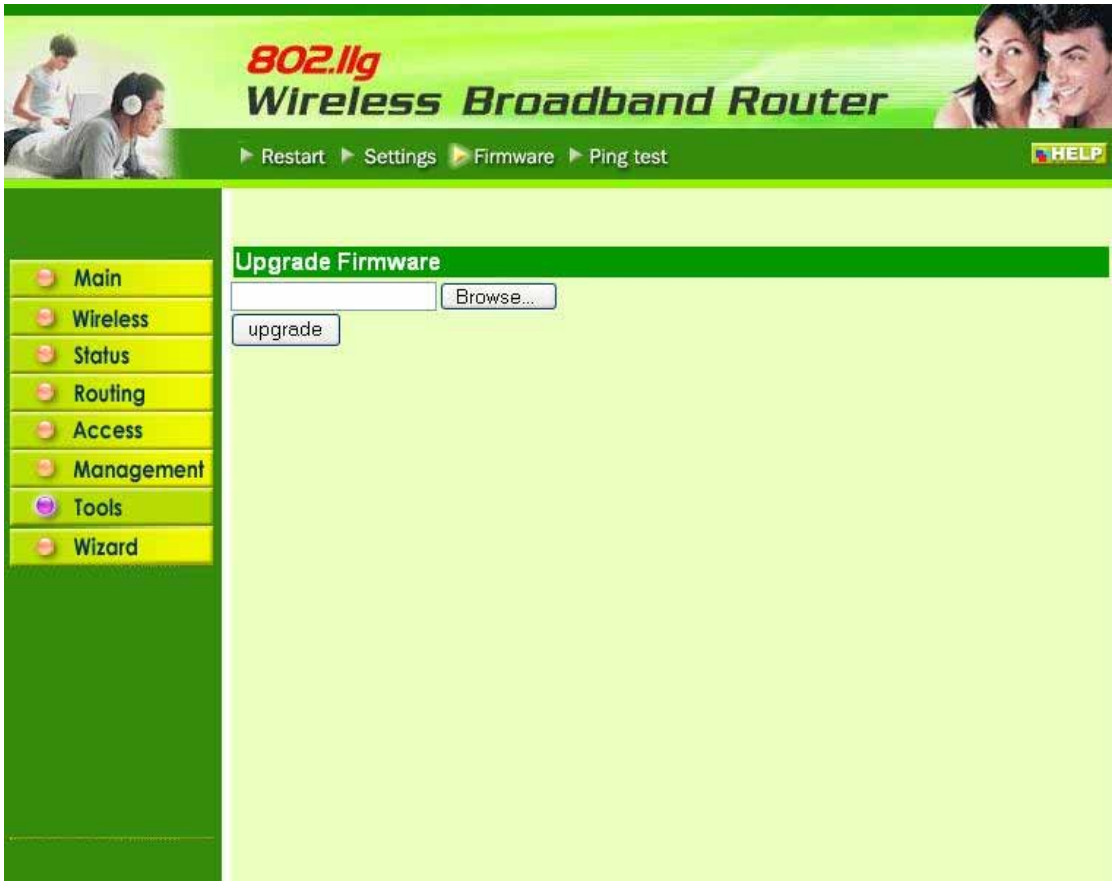
Save Settings: Click “Save” to save the current configuration as a profile that can load when necessary.

Load Settings: Click “Browse” and go to the location of a stored profile. Click “Load” to load the profile's settings.

Restore Factory Default Settings: Click “Restore” to restore the default settings. All configuration changes will lose.

2.7.3 Firmware

This screen enables user to keep the router firmware up to date.



Please follow the below instructions:

Download the latest firmware from the manufacturer's Web site, and save it to disk.

Click “Browse” and go to the location of the downloaded firmware file.

Select the file and click “Upgrade” to update the firmware to the latest release.

2.7.4 Ping Test

The ping test enables user to determine whether an IP address or host is present on the Internet. Type the host name or IP address in the text box and click Ping.

TECHNICAL SPECIFICATIONS

General	
Standards	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.11g; IEEE 802.11b
Protocol	CSMA/CD
Radio Technology	IEEE 802.11g Orthogonal Frequency Division Modulation
Data Transfer Rate	802.11b: 1, 2, 5.5, 11Mbps (auto sense) 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps @802.11g(auto sense) Ethernet: 10Mbps (half duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps (full- duplex)
Topology	Star
Receiver Sensitivity	54Mbps: Typical -70dBm @ 10% PER (Packet Error Rate) 11Mbps: Typical -85dBm @ 8% PER (Packet Error Rate)
TX Power	13dBm typically @ 802.11g 13dBm typically @ 802.11b
Network Cables	10BASE-T: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m) 100BASE-TX: 2-pair UTP Cat. 5 (100 m), EIA/TIA-568 100-ohm STP (100 m)
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Security	64/128-bits WEP Encryption; WPA, WPA-PSK
Channels	1 ~ 11 channels (FCC); 1 ~ 13 channels (ETSI); 1 ~ 14 channels (MKK)
Number of Ports	LAN: 4 x 10/100Mbps Auto-MDIX Fast Ethernet port WAN: 1 x 10/100Mbps Auto-MDIX Fast Ethernet port
Physical and Environmental	
DC inputs	DC 5V 2.5A
Power Consumption	3W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	147 x 115 x 35 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B